

INFORMATION SECURITY PROGRAM REGULATION



**DECEMBER 1978
DEPARTMENT OF DEFENSE**



POLICY

THE UNDER SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

November 2, 1978

FOREWORD

This Department of Defense Regulation governing the Information Security Program is issued under the authority of and pursuant to DoD Directive 5200.1, "Department of Defense Information Security Program," November 1978. It is applicable to all Department of Defense Components and activities without the necessity of further formal issuance by any DoD Component. Heads of DoD Components may issue supplementary instructions or directives necessary to provide for the internal administration of this Regulation within their respective Components.

This Regulation shall become effective on December 1, 1978, except that the provisions of paragraph 2-405b shall be effective immediately. This Regulation supersedes and cancels DoD 5200.1-R, November 1973, and Changes 1 and 2 thereto. Report Control Symbol DD-A (Q) 1183 is canceled.


Daniel J. Murphy
Deputy

CONTENTS

CHAPTER 1

GENERAL PROVISIONS

Section 1

REFERENCES

Paragraph	Page
1-100 References-----	I-1

Section 2

PURPOSE AND APPLICABILITY

1-200 Purpose-----	I-1
1-201 Applicability-----	I-1
1-202 Non-Government Operations-----	I-2
1-203 Combat Operations-----	I-2
1-204 Atomic Energy Material-----	I-2
1-205 Sensitive Compartmented and Communications Security Information-----	I-2
1-206 Automatic Data Processing Systems-----	I-2

Section 3

DEFINITIONS

1-300 Definitions-----	I-3
1-301 Classification Authority-----	I-3
1-302 Classification Guides-----	I-3
1-303 Classified Information-----	I-3
1-304 Classifier-----	I-3
1-305 Communications Security (COMSEC)-----	I-3
1-306 Component-----	I-4
1-307 Compromise-----	I-4
1-308 Critical Nuclear Weapon Design Information-----	I-4
1-309 Custodian-----	I-4
1-310 Declassification-----	I-4
1-311 Declassification Event-----	I-4
1-312 Derivative Classification-----	I-4

1-313	Document-----	I
1-314	Downgrade-----	I
1-315	Foreign Government Information-----	I
1-316	Formerly Restricted Data-----	I
1-317	Information-----	I
1-318	Information Security-----	I
1-319	Material-----	I
1-320	National Security-----	I
1-321	Original Classification-----	I
1-322	Regrade-----	I
1-323	Restricted Data-----	I
1-324	Sensitive Compartmented Information-----	I
1-325	Special Access Program-----	I
1-326	United States and Its Territories-----	I
1-327	Upgrade-----	I

Section 4

POLICIES

1-400	Classification-----	I
1-401	Declassification-----	I
1-402	Safeguarding-----	I

Section 5

SECURITY CLASSIFICATION DESIGNATIONS

1-500	General-----	I
1-501	"Top Secret"-----	I
1-502	"Secret"-----	I
1-503	"Confidential"-----	I

Section 6

AUTHORITY TO CLASSIFY, DOWNGRADE AND DECLASSIFY

1-600	Original Classification Authority-----	I
1-601	Derivative Classification Responsibility-----	I
1-602	Record and Report Requirements-----	I
1-603	Declassification and Downgrading Authority-----	I

CHAPTER II
CLASSIFICATION

Section 1

CLASSIFICATION RESPONSIBILITIES

2-100	Accountability of Classifiers-----	II-1
2-101	Classification Approval-----	II-1
2-102	Classification Planning-----	II-1
2-103	Challenges to Classification-----	II-2

Section 2

CLASSIFICATION PRINCIPLES, CRITERIA, AND CONSIDERATIONS

2-200	Reasoned Judgment -----	II-3
2-201	Identification of Specific Information-----	II-3
2-202	Specific Classifying Criteria-----	II-3
2-203	Presumption of Damage-----	II-4
2-204	Prohibitions-----	II-4
2-205	Classifying Scientific Research Data-----	II-5
2-206	Classifying Documents-----	II-5
2-207	Classifying Material Other Than Documents-----	II-6
2-208	State of the Art and Intelligence-----	II-6
2-209	Effect of Open Publication-----	II-6
2-210	Reevaluation of Classification Because of Compromise-----	II-6
2-211	Compilation of Information-----	II-7
2-212	Extracts of Information-----	II-7

Section 3

DURATION OF ORIGINAL CLASSIFICATION

2-300	General-----	II-8
2-301	Duration of Classification-----	II-8
2-302	Subsequent Extension of Duration of Classification-----	II-9

Section 4

CLASSIFICATION GUIDES

2-400	General-----	II-1
2-401	Multiservice Interest-----	II-1
2-402	Other Multiservice Interest Cases-----	II-1
2-403	Research, Development, Test and Evaluation-----	II-1
2-404	Project Phases-----	II-1
2-405	Review of Classification Guides-----	II-1
2-406	Distribution of Classification Guides-----	II-1
2-407	Index of Security Classification Guides-----	II-1

Section 5

RESOLUTION OF CONFLICTS

2-500	General-----	II-1
2-501	Procedures-----	II-1
2-502	Final Decision-----	II-1
2-503	Timing-----	II-1

Section 6

OBTAINING CLASSIFICATION EVALUATIONS

2-600	Procedures-----	II-14
-------	-----------------	-------

Section 7

INFORMATION DEVELOPED BY PRIVATE SOURCES

2-700	General-----	II-14
2-701	Patent Secrecy Act-----	II-15
2-702	Independent Research and Development-----	II-16
2-703	Other Private Information-----	II-16

Section 8

REGRADING

2-800	Raising to a Higher Level of Classification-----	II-16
2-801	Classification of Information Previously Determined to be Unclassified-----	II-17
2-802	Notification-----	II-17
2-803	Downgrading-----	II-17

Section 9

INDUSTRIAL OPERATIONS

2-900	Classification in Industrial Operations-----	II-17
2-901	Contract Security Classification Specification-----	II-17

CHAPTER III

DECLASSIFICATION AND DOWNGRADING

Section 1

GENERAL PROVISIONS

3-100	Policy-----	III-1
3-101	Responsibility of Officials-----	III-1
3-102	Exceptional Cases-----	III-1
3-103	Declassification by the Director of the Information Security Oversight Office-----	III-2

Section 2

SYSTEMATIC REVIEW

3-200	General-----	III-2
3-201	Systematic Review Guidelines-----	III-3
3-202	Systematic Review Procedures-----	III-3
3-203	Systematic Review of Classified Cryptologic Information-----	III-5

Section 3

MANDATORY REVIEW

3-300	Information Covered-----	III-5
3-301	Presidential Information-----	III-5
3-302	Submission of Requests for Review-----	III-6
3-303	Requirements for Processing-----	III-6
3-304	Foreign Government Information-----	III-7
3-305	Prohibition-----	III-7

Section 4

DECLASSIFICATION OF TRANSFERRED DOCUMENTS OR MATERIAL

3-400	Material Officially Transferred-----	III-8
3-401	Material Not Officially Transferred-----	III-8
3-402	Transfer for Storage or Retirement-----	III-8

Section 5

DOWNGRADING

3-500	Automatic Downgrading-----	III-9
3-501	Downgrading Upon Reconsideration-----	III-9

Section 6

MISCELLANEOUS

3-600	Notification of Changes in Declassification-----	III-9
3-601	Foreign Relations Series-----	III-9

CHAPTER IV

MARKING

Section I

GENERAL PROVISIONS

4-100	Designation-----	IV-1
4-101	Purpose of Designation-----	IV-1
4-102	Exception-----	IV-1
4-103	Documents or Other Material in General-----	IV-1
4-104	Identification of Classification Authority-----	IV-3
4-105	Wholly Unclassified Material-----	IV-3

Section 2

SPECIFIC MARKINGS ON DOCUMENTS

4-200	Overall and Page Marking-----	IV-4
4-201	Marking Components-----	IV-4
4-202	Portion Marking-----	IV-4
4-203	Compilations-----	IV-5
4-204	Subjects and Titles of Documents-----	IV-6
4-205	File, Folder, or Group of Documents-----	IV-6
4-206	Transmittal Documents-----	IV-6
4-207	Electronically Transmitted Messages-----	IV-6
4-208	Translations-----	IV-7

Section 3

MARKINGS ON SPECIAL CATEGORIES OF MATERIAL

4-300	General Provisions-----	IV-7
4-301	Charts, Maps and Drawings-----	IV-8
4-302	Photographs, Films and Recordings-----	IV-8
4-303	Decks of Accounting Machine Punched Cards-----	IV-9
4-304	Removable Automatic Data Processing and Word Processing Storage Media-----	IV-9
4-305	Documents Produced by ADP Equipment-----	IV-10
4-306	Material for Training Purposes-----	IV-10
4-307	Miscellaneous Material-----	IV-10
4-308	Special Access Program Documents and Material-----	IV-10
4-309	Associated Markings-----	IV-11

Section 4

CLASSIFICATION AUTHORITY, DURATION AND CHANGE MARKINGS

4-400	Declassification and Regrading Marking Procedures-----	IV-11
4-401	Applying Derivative Declassification Dates-----	IV-11
4-402	Commonly Used Markings-----	IV-14
4-403	Upgrading-----	IV-16
4-404	Limited Use of Posted Notice for Large Quantities of Material-----	IV-16

Section 5

ADDITIONAL WARNING NOTICES

4-500	General Provisions-----	IV-16
4-501	Restricted Data-----	IV-17
4-502	Formerly Restricted Data-----	IV-17
4-503	Intelligence Sources and Methods Information-----	IV-17
4-504	COMSEC Material-----	IV-17
4-505	Dissemination and Reproduction Notice-----	IV-18
4-506	Other Notations-----	IV-18

Section 6

REMARKING OLD MATERIAL

4-600	General-----	IV-18
4-601	Foreign Government Information-----	IV-18
4-602	Marking Documents or Material Marked "Subject to the General Declassification Schedule" or "Advanced Declassification Schedule"-----	IV-18
4-603	Marking Documents or Material Marked as "Exempt from the GDS" or Not Marked With Any Declassification Instructions-----	IV-19
4-604	Marking Documents or Material Marked "Group 4"-----	IV-19
4-605	Marking Material Marked Group 1, 2 or 3, or Not Group Marked-----	IV-20
4-606	Earlier Declassification-----	IV-20

CHAPTER V

SAFEKEEPING AND STORAGE

Section 1

STORAGE AND STORAGE EQUIPMENT

5-100	General Policy-----	V-1
5-101	Standards for Storage Equipment-----	V-1
5-102	Storage of Classified Information-----	V-1
5-103	Procurement and Phase-In of New Storage Equipment-----	V-3
5-104	Designations and Combinations-----	V-3
5-105	Repair of Damaged Security Containers-----	V-4

Section 2

CUSTODIAL PRECAUTIONS

5-200	Responsibilities of Custodians-----	V- 5
5-201	Care During Working Hours-----	V- 5
5-202	End-of-Day Security Checks-----	V- 6
5-203	Emergency Planning-----	V- 6
5-204	Telecommunications Conversations-----	V-10
5-205	Security of Meetings and Conferences-----	V-10

CHAPTER VI

COMPROMISE OF CLASSIFIED INFORMATION

6-100	Policy-----	VI-1
6-101	Cryptographic Information-----	VI-1
6-102	Responsibility of Discoverer-----	VI-1
6-103	Preliminary Inquiry-----	VI-1
6-104	Investigation-----	VI-2
6-105	Responsibility of Authority Ordering Investigation-----	VI-2
6-106	Responsibility of Originator-----	VI-2
6-107	Espionage and Deliberate Compromise-----	VI-3
6-108	Unauthorized Absentees-----	VI-3

CHAPTER VII

ACCESS, DISSEMINATION AND ACCOUNTABILITY

Section 1

ACCESS

7-100	Policy-----	VII-1
7-101	Determination of Trustworthiness-----	VII-1
7-102	Continuous Evaluation of Eligibility-----	VII-2
7-103	Determination of Need-to-Know-----	VII-2
7-104	Revocation of Security Clearance for Cause-----	VII-2
7-105	Access by Persons Outside the Executive Branch-----	VII-2
7-106	Access by Foreign Nationals, Foreign Governments, International Organizations, and Immigrant Aliens-----	VII-5
7-107	Other Situations-----	VII-6
7-108	Access Required by Other Executive Branch Investi- gative and Law Enforcement Agents-----	VII-6

Section 2

DISSEMINATION

7-200	Policy-----	VII-6
7-201	Restraints on Special Access Requirements-----	VII-7
7-202	Information Originating in a Non-DoD Department or Agency-----	VII-7
7-203	Foreign Intelligence Information-----	VII-7
7-204	Restricted Data and Formerly Restricted Data-----	VII-7
7-205	NATO and CENTO Information-----	VII-7
7-206	COMSEC Information-----	VII-7
7-207	Dissemination of Top Secret Information-----	VII-7
7-208	Dissemination of Secret and Confidential Information-----	VII-7
7-209	Restraint on Reproduction-----	VII-8
7-210	Code Words, Nicknames and Exercise Terms-----	VII-8
7-211	Scientific and Technical Meetings-----	VII-8

Section 3

ACCOUNTABILITY AND CONTROL

7-300	Top Secret Information-----	VII- 9
7-301	Secret Information-----	VII-10
7-302	Confidential Information-----	VII-10
7-303	Receipt of Classified Material-----	VII-10
7-304	Working Papers-----	VII-10

CHAPTER VIII-

TRANSMISSION

Section 1

METHODS OF TRANSMISSION OR TRANSPORTATION

8-100	Policy-----	VIII-1
8-101	Top Secret Information-----	VIII-1
8-102	Secret Information-----	VIII-2
8-103	Confidential Information-----	VIII-3
8-104	Transmission of Classified Information to Foreign Governments-----	VIII-4
8-105	Consignor-Consignee Responsibility for Shipment of Bulky Material-----	VIII-5
8-106	Transmission of Communications Security (COMSEC) Information-----	VIII-6
8-107	Transmission of Restricted Data-----	VIII-7

Section 2

PREPARATION OF MATERIAL FOR TRANSMISSION OR SHIPMENT

8-200	Envelopes or Containers-----	VIII-7
8-201	Addressing-----	VIII-8
8-202	Receipt Systems-----	VIII-9
8-203	Exceptions-----	VIII-9

Section 3

RESTRICTIONS, PROCEDURES AND AUTHORIZATION CONCERNING ESCORT/

HAND-CARRYING OF CLASSIFIED INFORMATION

8-300	General Restrictions-----	VIII-9
8-301	Restrictions on Hand-carrying Classified Information Aboard Commercial Passenger Aircraft-----	VIII-10
8-302	Procedures for Hand-carrying Classified Information Aboard Commercial Passenger Aircraft-----	VIII-11
8-303	Authority to Approve Escort/Hand-carry of Classified Information-----	VIII-14

CHAPTER IX

DISPOSAL AND DESTRUCTION

9-100	Policy-----	IX-1
9-101	Methods of Destruction-----	IX-1
9-102	Records of Destruction-----	IX-1
9-103	Classified Waste-----	IX-1

CHAPTER X

SECURITY EDUCATION

10-100 Responsibility and Objectives-----	X-1
10-101 Scope and Principles-----	X-1
10-102 Refresher Briefings-----	X-2
10-103 Foreign Travel Briefing-----	X-2
10-104 Debriefings-----	X-2

CHAPTER XI

FOREIGN GOVERNMENT INFORMATION

Section 1

CLASSIFICATION

11-100 Classification-----	XI-1
11-101 Duration of Classification-----	XI-1

Section 2

DECLASSIFICATION

11-200 Policy-----	XI-2
11-201 Systematic Review-----	XI-2
11-202 Mandatory Review-----	XI-2

Section 3

MARKING

11-300 Equivalent United States Classification Designations-----	XI-3
11-301 Marking NATO and CENTO Documents-----	XI-3
11-302 Marking Other Foreign Government Documents-----	XI-3
11-303 Marking of DoD Classification Determinations-----	XI-4
11-304 Marking of Foreign Government Information in DoD Documents-----	XI-4

Section 4

PROTECTIVE MEASURES

11-400 NATO and CENTO Classified Information-----	XI-5
11-401 Other Foreign Government Information-----	XI-5

CHAPTER XII

SPECIAL ACCESS PROGRAMS

12-100 Policy-----	XII-1
12-101 Establishment of Special Access Programs-----	XII-1
12-102 Reporting on Special Access Programs-----	XII-2
12-103 Review, Continuation and Accounting for Special Access Programs-----	XII-2
12-104 Notification-----	XII-3

CHAPTER XIII

PROGRAM MANAGEMENT

Section 1

EXECUTIVE BRANCH OVERSIGHT AND POLICY DIRECTION

13-100 National Security Council-----	XIII-1
13-101 Administrator of General Services-----	XIII-1
13-102 Information Security Oversight Office-----	XIII-1
13-103 Interagency Information Security Committee-----	XIII-2

Section 2

DEPARTMENT OF DEFENSE

13-200 Management Responsibility-----	XIII-2
13-201 DoD Information Security Committee-----	XIII-3

Section 3

DOD COMPONENTS

13-300 General-----	XIII-3
13-301 Military Departments-----	XIII-3
13-302 Other Components-----	XIII-4
13-303 Program Monitorship-----	XIII-4
13-304 Field Program Management-----	XIII-4

Section 4

REPORTS REQUIREMENTS

13-400 Reports Requirements-----	XIII-4
----------------------------------	--------

CHAPTER XIV

ADMINISTRATIVE SANCTIONS

14-100 Individual Responsibility-----	XIV-1
14-101 Violations Subject to Sanctions-----	XIV-1
14-102 Corrective Action-----	XIV-1
14-103 Administrative Discrepancies-----	XIV-1
14-104 Reporting Violations-----	XIV-2

APPENDICES

Appendix A - Equivalent Foreign and International Pact Organization Security Classifications-----	A1
Appendix B - General Accounting Office Officials Authorized to Certify Security Clearances-----	B1
Appendix C - Instructions Governing Use of Code Words, Nicknames, and Exercise Terms-----	C1
Appendix D - Federal Aviation Administration Air Transportation Security Field Offices-----	D1

ENCLOSURES

Enclosure 1 - References-----	
-------------------------------	--

DEPARTMENT OF DEFENSE INFORMATION SECURITY PROGRAM REGULATION

CHAPTER I

GENERAL PROVISIONS

Section 1

REFERENCES

1-100 References

- (a) DoD Directive 5200.1, "DoD Information Security Program," dated November 1978.
- (b) Executive Order 12065, "National Security Information," dated June 28, 1978
- (c) "Information Security Oversight Office Directive No. 1 Concerning National Security Information," dated October 2, 1978
- (d) and all others are at enclosure 1

Section 2

PURPOSE AND APPLICABILITY

1-200 Purpose

It is the purpose of this Regulation to ensure that information of the Department of Defense relating to national security is protected, but only to the extent and for such period as is necessary. This Regulation establishes a system for classification, downgrading and declassification of information; sets forth policies and procedures to safeguard such information; and provides for oversight and enforcement.

1-201 Applicability

This Regulation governs the Department of Defense Information Security Program and takes precedence over all Component regulations which implement that Program. In accordance with the provisions of references (a), (b), and (c) above, it establishes, for uniform application throughout the Department of Defense, the policies, standards, criteria and procedures for the security classification, downgrading, declassification and safeguarding of information that is owned by, produced for or by, or under the control of the Department of Defense or the Components thereof.

1-202 Non-Government Operations

Except as otherwise provided herein, the provisions of this Regulation shall be made applicable by contract, or other legally binding instrument, to operations of nongovernment personnel entrusted with classified information. (See references (k), (aa) and (ab)).

1-203 Combat Operations

The provisions of this Regulation relating to accountability, dissemination, transmission, or safeguarding of classified information may be modified by military commanders but only to the extent necessary to meet local conditions in connection with combat or combat-related operations. Classified information should be introduced into forward combat areas or zones or areas of potential hostile activity only to the extent essential to accomplishment of the military mission.

1-204 Atomic Energy Material

Nothing in this Regulation supersedes any requirement related to "Restricted Data" in the Atomic Energy Act of August 30, 1954, as amended, or the regulations of the Department of Energy under that Act. "Restricted Data" and material designated as "Formerly Restricted Data," shall be handled, protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act and the regulations issued pursuant thereto.

1-205 Sensitive Compartmented and Communications Security Information

Sensitive Compartmented Information (SCI) and communications security (COMSEC) information shall be handled and controlled in accordance with applicable national and departmental directives and instructions. Other classified information, while in established SCI or COMSEC areas, may be handled in the same manner as SCI or COMSEC information. Classification principles and procedures, markings, downgrading, and declassification actions prescribed in this Regulation apply to SCI and COMSEC information. (See also Paragraph 13-200c).

1-206 Automatic Data Processing Systems

This Regulation applies to protection of classified information processed, stored or used in, or communicated, displayed or disseminated by an automatic data processing (ADP) system. Additional security policy, responsibilities, and requirements applicable specifically to ADP systems are contained in references (al) and (am).

DEFINITIONS

1-300 Definitions

As used herein, the following terms and meanings shall be applicable.

1-301 Classification Authority

The authority vested in an official of the Department of Defense to classify originally information or material that, pursuant to the provisions of this Regulation, is determined by that official to require protection against unauthorized disclosure in the interest of national security. It is also the authority to prolong classification, within the limits prescribed by the Regulation, only so long as the basis for original classification remains.

1-302 Classification Guides

Guidance issued or approved by an original Top Secret classification authority that identifies information or material to be protected from unauthorized disclosure and specifies the level and duration of classification assigned or assignable to such information or material under authority of reference (b). For purposes of this Regulation, this term does not include DD Form 254, "Contract Security Classification Specification."

1-303 Classified Information

Information or material that is: (i) owned by, produced for or by, or under the control of the United States Government, and (ii) determined pursuant to Executive Order 12065 or prior orders and this Regulation to require protection against unauthorized disclosure, and (iii) so designated.

1-304 Classifier

An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

1-305 Communications Security (COMSEC)

The protection resulting from any measures taken to: (i) deny unauthorized persons information related to national security that might be derived from telecommunications, or (ii) to ensure the authenticity of such telecommunications.

1 306 Component

The Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies.

1-307 Compromise

The disclosure of classified information to persons not authorized access thereto.

1-308 Critical Nuclear Weapon Design Information

That Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munition or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components which DoD personnel act, maintain, operate, test, or replace.

1-309 Custodian

An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

1-310 Declassification

The determination that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized disclosure, together with a removal or cancellation of the classification designation.

1-311 Declassification Event

An event that eliminates the need for continued classification of information.

1-312 Derivative Classification

A determination that information is in substance the same as information that is currently classified, and a designation of the level of classification.

1-313 Document

Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings,

1-314 Downgrade

A determination that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such lower degree of protection.

1-315 Foreign Government Information

Information that is (i) provided to the United States by a foreign government or international organization of governments in the expectation, express or implied, that the information is to be kept in confidence; or (ii) produced by the United States pursuant to a written joint arrangement with a foreign government or international organization of governments requiring that either the information or the arrangement, or both, be kept in confidence. Such a written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record.

1-316 Formerly Restricted Data

Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as Restricted Data.

1-317 Information

Knowledge that can be communicated by any means.

1-318 Information Security

The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order or statute.

1-319 Material

Any product or substance on, or in which, information is embodied.

1-320 National Security

The national defense and foreign relations of the United States.

1-321 Original Classification

An initial determination that information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made.

1-322 Regrade

A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection.

1-323 Restricted Data

All data concerning (i) design, manufacture or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act. (See also Section 11y, Atomic Energy Act of 1954, as amended, and "Formerly Restricted Data," paragraph 1-316.)

1-324 Sensitive Compartmented Information

All information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

1-325 Special Access Program

Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements, special designation of officials authorized to determine "need-to-know," or special lists of persons determined to have a "need-to-know."

1-326 United States and Its Territories

The 50 States; the District of Columbia; the Commonwealth of Puerto Rico; the Territories of Guam, American Samoa, and the Virgin Islands; the Trust Territory of the Pacific Islands; the Canal Zone; and the Possessions, Midway and Wake Islands.

1-327 Upgrade

A determination that certain classified information requires, in the interests of national security, a higher degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such higher degree.

Section 4

POLICIES

1-400 Classification

a. Basic Policy. Except as provided in the Atomic Energy Act of 1954, as amended, Executive Order 12065, as implemented by reference (c) and this Regulation, provides the only basis for classifying information. It is the policy of the Department of Defense to make available to the public as much information concerning its activities as possible consistent with the need to protect the national security. Accordingly, security classification shall be applied only to protect the national security.

b. Resolution of Doubts. Unnecessary classification and higher than necessary classification shall be scrupulously avoided. If there is reasonable doubt which designation of security classification is appropriate, or whether information or material should be classified at all, the less restrictive treatment should be used.

c. Duration. Classification shall not be continued longer than necessary for the protection of national security. Each decision to classify requires a simultaneous determination of the duration such classification must remain in force.

1-401 Declassification

Declassification of information shall be given emphasis comparable to that accorded to classification. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or upon the occurrence of a declassification event.

1-402 Safeguarding

Information classified under the provisions of this Regulation shall be afforded the level of protection against unauthorized disclosure commensurate with the level of classification assigned under the varying conditions which may arise in connection with its use, dissemination, storage, movement or transmission, and destruction.

SECURITY CLASSIFICATION DESIGNATIONS

1-500 General

Information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of three designations, namely: "Top Secret," "Secret," or "Confidential." The markings "For Official Use Only," and "Limited Official Use" shall not be used to identify classified information. Moreover, no other term such as "Sensitive," "Conference," or "Agency" shall be used in conjunction with the authorized classification designations.

1-501 "Top Secret"

"Top Secret" shall be applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

1-502 "Secret"

"Secret" shall be applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

1-503 "Confidential"

"Confidential" shall be applied to information or material the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security. Examples of "identifiable damage" include the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; revelation of performance characteristics, test data, design, and production data on munitions of war.

AUTHORITY TO CLASSIFY, DOWNGRADE AND DECLASSIFY

1-600 Original Classification Authority

a. Control. Authority for original classification of information as Top Secret, Secret or Confidential may be exercised only by the Secretary of Defense, the Secretaries of the Military Departments, and by officials to whom such authority is specifically delegated in accordance with and subject to the restrictions of this Section of the Regulation. In the absence of an original classification authority, the person designated to act in his or her absence may exercise the classifier's authority.

b. Delegation of Classification Authority. Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide. Delegations of original classification authority shall be limited to the minimum number required for efficient administration and to those officials whose duties involve the origination and evaluation of information warranting classification at the level stated in the delegation.

1. Top Secret. Only the Secretary of Defense and the Secretaries of the Military Departments may delegate original Top Secret classification authority. Such delegation may only be made to principal subordinate officials who are determined by the respective Secretaries to have frequent need to exercise such authority. The delegation of authority shall include specific notice as to whether the Top Secret classification authority is authorized to delegate original Secret and Confidential classification authority.

2. Secret and Confidential. Only the Secretary of Defense, the Secretaries of the Military Departments, and officials with original Top Secret classification authority authorized to do so, may delegate original Secret and Confidential classification authority to subordinate officials whom they respectively determine to have frequent need to exercise such authority.

3. Each delegation of original classification authority shall be in writing and shall specify the title of the position held by the recipient.

4. Officials to whom original classification authority is delegated may not redelegate such authority.

c. Restrictions. Only the Secretary of Defense, the Secretaries of the Military Departments and those officials specifically designated to act for them in their absence are authorized to prolong the duration of classification beyond 20 years from the date of original classification.

Other officials designated to exercise original classification authority, pursuant to this Regulation, are authorized to prolong classification as follows:

1. Except as provided in paragraph 3., below, original Top Secret classification authorities may prolong classification not more than 20 years from the date of original classification.
2. Original Secret and Confidential classification authorities may prolong classification not more than 6 years from the date of original classification.
3. The classification of foreign government information may be prolonged by an original Top Secret classification authority up to 30 years from the date of original classification or the date it was acquired or classified by the United States, whichever is earlier.

d. Requests for Classification Authority

1. A request for the delegation of original classification authority shall be made only when the following conditions exist:

(a) The normal course of operations or missions of the organization is such as to result in the origination of information warranting classification,

(b) There is a substantial degree of local autonomy in operations or missions as distinguished from dependence upon a higher level of command or supervision for relatively detailed guidance.

(c) There is adequate knowledge by the originating level to make sound classification determinations as distinguished from having to seek such knowledge from a higher level of command or supervision.

(d) There is a valid reason why already designated classification authorities in the originator's chain of command or supervision have not issued or cannot issue classification guidance sufficient to meet the originator's normal needs.

2. Each request for a delegation of original classification authority shall:

(a) Identify the title of the position held by the nominee and the nominee's organization;

(b) Contain a description of the circumstances, consistent with 1., above, which justifies the delegation of such authority; and

(c) Be submitted through established channels to the Secretary of Defense, the Secretary of the appropriate Military Department, or the appropriate Top Secret classification authority authorized to act on such requests. (See paragraph 1-602.)

01 Derivative Classification Responsibility

Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form, information which is already classified or those who apply markings in accordance with guidance from an original classification authority. Persons who apply derivative classifications should take care to determine whether their paraphrasing, restating or summarizing of classified information has removed all or part of the basis for classification. Persons who apply such derivative classification markings shall:

- a. Respect original classification decisions;
- b. Verify the information's current level of classification so far as practicable before applying the markings; and
- c. Carry forward to any newly created documents the assigned dates and events for declassification or review and any additional authorized markings. Where checks with originators or other appropriate inquiries reveal that no classification or a lower classification than originally assigned is appropriate, the information shall be marked accordingly.

02 Record and Report Requirements

- a. Records of designations of original classification authority shall be maintained as follows:

1. Top Secret Authorities. A current listing by title and organization of officials designated to exercise original Top Secret classification authority shall be maintained by:

- (a) The Office of the Deputy Under Secretary of Defense (Policy) for the Office of the Secretary of Defense; the Organization of the Joint Chiefs of Staff; the Headquarters of each Unified Command; the Headquarters of Subordinate Joint Commands; and the Defense Agencies.

- (b) The Offices of the Secretaries of the Military Departments for the officials of their respective departments, including Unified Commands but excluding officials from their respective departments who are serving in Headquarters elements of Unified Commands and Headquarters of Joint Commands subordinate thereto.

2. Secret and Confidential Authorities. A current listing by title and organization of officials designated to exercise original Secret and Confidential classification authority shall be maintained by:

- (a) The Office of the Deputy Under Secretary of Defense (Policy) and the Office of the Secretary of Defense.

(b) The offices of the Secretaries of the Military Departments for the officials of their respective departments, including Specified Commands but excluding officials from their respective departments who are serving in Headquarters elements of Unified Commands and Headquarters elements of Joint Commands subordinate thereto.

(c) The Director, Joint Staff, for the Organization of the Joint Chiefs of Staff.

(d) The Commanders-in-Chief of the Unified and Specified Commands, for their respective Headquarters and the Headquarters of Subordinate Joint Commands.

(e) The Directors of the Defense Agencies, for their respective agencies.

3. If the listing of titles of positions and organizations prescribed in subparagraphs 1 and 2 above discloses intelligence or other information that either qualifies for security classification protection or otherwise qualifies to be withheld from public release under statute, some other means may be recommended by the DoD component by which original classification authorities can be readily identified. Such recommendation shall be submitted to the Office of the Deputy Under Secretary of Defense (Policy) for approval.

4. The listings prescribed in subparagraphs 1 and 2 above shall be reviewed at least annually by the senior official designated in or pursuant to paragraphs 13-200a, 13-301 or 13-302 or his or her designee to ensure that officials so listed have demonstrated a continuing need to exercise original classification authority.

b. The DoD Components that maintain listings of designated original classification authorities shall, upon request, submit copies of such listings to the Office of the Deputy Under Secretary of Defense (Policy).

1-603 Declassification and Downgrading Authority

a. Authority to declassify and downgrade information classified under provisions of this Regulation shall be exercised as follows:

1. By the Secretary of Defense and the Secretaries of the Military Departments, with respect to all information over which their respective Departments exercise final classification jurisdiction;

2. By the official who authorized the original classification, if that official is still serving in the same position, by a successor, or by a supervisory official of either; and

3. By other officials designated for the purpose in accordance with subparagraph b., below.

b. The Secretary of Defense, the Secretaries of the Military Departments, or their designees shall designate additional officials at the lowest practicable echelons of command and supervision to exercise declassification and downgrading authority over classified information in their functional areas of interest. Records of officials so designated shall be maintained in the same manner as is prescribed in paragraph 1-602.a.1. for records of designations of original classification authority.

CHAPTER II

CLASSIFICATION

Section 1

CLASSIFICATION RESPONSIBILITIES

2-100 Accountability of Classifiers

a. Classifiers are accountable for the propriety of the classifications they assign, whether by exercise of original classification authority or by derivative classification.

b. An official who classifies a document or other material and is identified thereon as the classifier is and continues to be an accountable classifier even though the document or material is finally approved or signed at a higher level in the same organization. (See paragraph 4-104.)

2-101 Classification Approval

a. When an official signs or finally approves a document or other material already marked to reflect a particular level of classification, he or she shall review the information contained therein to determine if the classification markings are appropriate. If, in his or her judgment, the classification markings are not supportable, he or she shall, at that time, cause such markings to be removed or changed as appropriate to reflect accurately the classification of the information involved.

b. A higher level official through or to whom a document or other material passes for signature or final approval becomes jointly responsible with the accountable classifier for the classification(s) assigned. Such official has discretion to decide whether his subordinates who have classification authority shall be identified as accountable classifier when they have exercised that authority.

2-102 Classification Planning

a. Advance classification planning is an essential part of the development of any plan, operation, program, research and development project, or procurement action that involves classified information. Classification aspects must be considered from the outset to assure adequate protection for the information and for the activity itself, and to eliminate impediments to the execution or implementation of the plan, operations order, program, project or procurement action.

b. The commander or official charged with the development of any plan, program or project, in which classification is a factor, shall include therein, under a clearly identifiable title or heading, classification guidance covering the information involved in that effort. The guidance shall conform to the requirements contained in Section 4 of this Chapter.

2-103 Challenges to Classification

If holders of classified information have substantial reason to believe that the information is classified improperly or unnecessarily or that an overly restrictive period for continued classification has been assigned, they are encouraged to discuss such classification with their security manager (paragraph 13-304) or the classifier of the information with a view to bringing about corrections if appropriate. Alternatives are set out below in the event the holder desires to pursue the challenge formally.

a. Each DoD Component will establish, as part of its information security program, procedures whereby holders of classified information may challenge the decision of the classifier of the information. Each Component will designate one or more offices to which challenges to classification and appeals therefrom may be submitted. Its procedures shall provide for preservation of the anonymity of the challenger. These procedures shall be publicized within the Component through its supplement to this Regulation or other suitable publication.

b. Challenges to classification made under the provisions of this paragraph shall include sufficient description of the information or document being challenged to permit identification of the information or document and the classifier thereof with reasonable effort. Challenges to classification shall also include the reason(s) why the challenger believes that the information is classified improperly or unnecessarily or that an overly restrictive period for continued classification has been assigned.

c. Challenges received under the provisions of this paragraph will be acted upon within thirty days of receipt. The challenger shall be notified of any changes made as a result of the challenge or the reasons why no change is made. Such notice shall, in appropriate cases, advise the challenger that, within thirty days, the decision may be appealed to an official designated by the Component for that purpose.

d. Within thirty days after receipt of an appeal, the designated official will consider the appeal, requesting additional information as necessary from either the challenger or classifier and may reverse, amend or uphold the initial decision of the classifier, informing both the challenger and classifier of the determination made as well as the option of further appeal to the Defense or Military Department Information Security Committee, as appropriate (see paragraphs 13-201 and 13-301, respectively).

e. Pending final determination of a challenge to classification and appeal, the information or document in question shall be safeguarded as required for the level of classification initially assigned.

f. The fact that an employee or military member of the Department of Defense has issued a challenge to classification shall not in any way result in or serve as a basis for adverse personnel action.

g. The provisions of this paragraph do not apply to or affect declassification review actions undertaken under the mandatory review requirements of Section 3, Chapter III of this Regulation or under the provisions of DoD Directive 5400.7, reference (q).

Section 2

CLASSIFICATION PRINCIPLES, CRITERIA, AND CONSIDERATIONS

2-200 Reasoned Judgment

Reasoned judgment shall be exercised in making classification decisions. A positive basis must exist for classification. Both advantages and disadvantages of classification must be weighed. If, after consideration of the provisions of this Section of the Regulation, there is reasonable doubt whether the information in question should be classified at all, the information should not be classified.

2-201 Identification of Specific Information

Before a classification determination is made, each item of information that may require protection shall be identified exactly. This requires identification of that specific information which comprises the basis for a particular national advantage or advantages which, if the information were compromised, would or could be damaged, minimized, or lost, thereby adversely affecting the national security.

2-202 Specific Classifying Criteria

A determination to classify shall be made only by an original classification authority and only when, first, the information is within categories (a) through (g), below; and second, the unauthorized disclosure of the information reasonably could be expected to cause at least identifiable damage to the national security. The determination involved in the first step is separate and distinct from that in the second. The fact that the information falls under one or more of the criteria shall not be presumed to mean that the information automatically meets the damage criteria. Information may not be considered for classification unless it concerns:

- a. military plans, weapons, or operations;

- b. foreign government information;
- c. intelligence activities, sources or methods;
- d. foreign relations or foreign activities of the United States;
- e. scientific, technological, or economic matters relating to the national security;

f. United States Government programs for safeguarding nuclear materials or facilities; or

g. other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the Secretary of Defense or Secretaries of the Military Departments. Recommendations concerning the need to designate additional categories of information that may be considered for classification shall be forwarded through channels to the appropriate Secretary for determination. Each such determination shall be reported promptly to the Director for Information Security, Office of the Deputy Under Secretary of Defense (Policy), for promulgation in an Appendix to this Regulation and reporting to the Director of the Information Security Oversight Office.

2-203 Presumption of Damage

Unauthorized disclosure of foreign government information (see paragraph 11-100) or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security.

2-204 Prohibitions

a. Classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.

b. Basic scientific research information not clearly related to the national security may not be classified.

c. A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified until and unless the government acquires a proprietary interest in the product. This prohibition does not affect the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-188). (See Section 7, this Chapter.)

d. References to classified documents that do not disclose classified information may not be classified or used as a basis for classification.

e. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of Executive Order 12065 and this Regulation or to prevent or delay the public release of such information.

f. No document originated on or after 1 December 1978 may be classified after receipt of a request for the document under the Freedom of Information Act or the Mandatory Review provisions of this Regulation (Section 3, Chapter III) unless such classification is consistent with this Regulation and is authorized by the Secretary or Deputy Secretary of Defense or by the Secretaries or Under Secretaries of the Military Departments. Documents originated before 1 December 1978 and subject to such a request may not be classified unless such classification is consistent with this Regulation and is authorized by an official with Top Secret classification authority. Classification authority under this provision shall be exercised personally, on a document-by-document basis and subject to the provisions of paragraph 2-801.

g. Classification may not be restored to documents containing information already declassified and released to the public under this or prior Regulations.

h. A compilation of official public releases may not be classified.

2-205 Classifying Scientific Research Data

Ordinarily, except for information which meets the definition of Restricted Data, basic scientific research or results thereof shall not be classified. However, classification would be appropriate if the information concerns an unusually significant scientific "breakthrough" and there is sound reason to believe it is not known or within the state-of-the-art of other nations, and it supplies the United States with an advantage directly related to national security.

2-206 Classifying Documents

Each document and portion thereof shall be classified on the basis of the information it contains or reveals. The fact that a document makes reference to a classified document is not a basis for classification unless the reference, standing alone, reveals classified information. (See paragraph 2-204d.) The overall classification of a document, file folder, or group of physically-connected documents shall be at least as high as that of the most highly classified component. The subject or title of a classified document should normally be unclassified. When the information revealed by a subject or title warrants classification, an unclassified short title shall be added for reference purposes.

2-207 Classifying Material Other Than Documents

a. Items of equipment or other physical objects may be classified only when classified information may be derived from them by visual observation of their internal or external appearance or structure, or of an operation, test, application or use of such objects. The overall classification assigned to end items of equipment or objects shall be at least as high as the highest classification of any of its integrated parts.

b. If mere knowledge of the existence of the item of equipment or object would compromise or nullify its national security advantage, its existence would warrant classification.

2-208 State of the Art and Intelligence

Classification requires consideration of the information available from intelligence sources concerning the extent to which the same or similar information is known or is available to others. It is also important to consider whether it is known, publicly or internationally, that the United States has the information or even is interested in the subject matter. The state of the art in other nations may often be a vital consideration.

2-209 Effect of Open Publication

Appearance in the public domain of information currently classified or being considered for classification does not preclude initial or continued classification; however, such disclosures require immediate reevaluation of the information to determine whether the publication has so compromised the information that downgrading or declassification is warranted. Similar consideration must be given to related items of information in all programs, projects or items incorporating or pertaining to the compromised items of information. In these cases, if the release is shown to have been made or authorized by an official of the Executive Branch authorized to declassify and release such information, classification of clearly identified items shall no longer be continued. However, holders should continue classification until advised to the contrary by a competent Government authority.

2-210 Reevaluation of Classification Because of Compromise

Classified information, and information related thereto, that is or may have been compromised, shall be reevaluated and acted upon as follows:

a. The original classifying authority, upon learning that a compromise or probable compromise of specific classified information has occurred, shall:

1. Reevaluate the information involved and determine whether: (a) the classification should be continued without changing the specific information involved; (b) the specific information, or parts thereof, should be modified to minimize or nullify the effects of the reported compromise and the classification retained; (c) declassification or downgrading is warranted.

2. When such determination is within categories (b) or (c) of subparagraph 1., above, give prompt notice thereof to all holders of such information.

b. Upon learning that a compromise or probable compromise has occurred, any official having original classification jurisdiction over related information shall reevaluate the related information and determine whether one of the courses of action enumerated in paragraph a.1., above, should be taken or, in lieu thereof, upgrading of the related information is warranted. When such a determination is within categories (b) or (c) of paragraph a.1., above, or that upgrading of the related items is warranted, prompt notice of the determination shall be given to all holders of the related information. (See Chapter VI.)

2-211 Compilation of Information

A compilation of unclassified items of information shall normally not be classified. In unusual circumstances, classification may be required if the combination of unclassified items of information provides an added factor which warrants classification under paragraph 2-202. Classification on this basis shall be used sparingly and shall be fully supported by a written explanation which will be provided with the material so classified. (See also paragraphs 2-204 and 4-203.)

2-212 Extracts of Information

Information extracted from a classified source will be derivatively classified, or not classified, as the case may be, in accordance with the classification markings shown in the source. The overall marking and internal marking of the source should supply adequate classification guidance to the person making the extraction. If internal markings or classification guidance are not found in the source and no reference is made to an applicable classification guide that is available for use by the person making the extraction, the extracted information will be classified according to either the overall marking of the source, or guidance obtained from the classifier of the source material.

DURATION OF ORIGINAL CLASSIFICATION

2-300 General

At the time a determination is made by an official with authority to originally classify information as Top Secret, Secret or Confidential, a simultaneous decision must be made by that official as to the duration of time such classification must remain in force. In arriving at the latter decision, the classifier must exercise careful judgment as to how far in the future the basis for original classification will remain valid. Only in cases where a specific determination has been made that earlier declassification should not be accomplished, may original classification authorities specify declassification dates or events at the limit of their authority as prescribed in paragraph 1-600c of this Regulation.

2-301 Duration of Classification

a. Information shall be classified only so long as its unauthorized disclosure would result in at least identifiable damage to the national security. Any willful extension beyond that period is a violation of this Regulation.

b. Dates or events on which automatic declassification should occur shall be as early as possible consistent with the national security and, except as provided in paragraph c., below, shall be no more than six years from the date of original classification. Any event specified for the determination of declassification shall be an event certain to occur.

c. Classification may be prolonged for more than six years only by officials designated as original Top Secret classification authorities. This authority shall be used only when such officials determine that the two conditions specified in paragraph 2-202 for original classification will continue throughout the entire period the classification will be in effect and only for the following reasons:

1. The information is "foreign government information" as defined in this Regulation;
2. The continuing protection of the information is specifically required by statute;
3. The continuing protection of the information is essential to the national security because it reveals intelligence sources or methods which, if lost, cannot be regained or replaced promptly;
4. The continuing protection of the information is essential to the national security because it pertains to communications security;

5. The information reveals vulnerability or capability data the unauthorized disclosure of which can reasonably be expected to result in nullifying the effectiveness of a system, installation or project important to the national security;

6. The information concerns plans important to national security the unauthorized disclosure of which can reasonably be expected to result in nullifying the effectiveness of the plan itself or impeding its orderly implementation;

7. The information concerns specific foreign relations matters the continued protection of which is essential to the national security; or

8. Disclosure of the information would place a person in immediate jeopardy.

d. A Top Secret classification authority who prolongs a classification for more than six years shall set a specific date or event for declassification or a specific date for review for declassification which shall be as early as possible consistent with the national security and subject to the following limitations:

1. The date or event may not be more than twenty years from the date of original classification;

2. A twenty-year declassification review date may be set only when consistent with the guidelines promulgated pursuant to paragraph 3-201 of this Regulation (see also Chapter XI, Foreign Government Information); and

3. When classification is extended for more than six years, the identity of the original Top Secret classification authority and reasons for the extension of classification will be recorded as prescribed by paragraph 4-103 of this Regulation.

2-302 Subsequent Extension of Duration of Classification

The duration of classification specified at the time of original classification may be extended only by officials with requisite original classification authority and only if all known holders of the information can be notified of such action prior to the date or event previously set for declassification.

CLASSIFICATION GUIDES

2-400 General

a. A classification guide shall be issued for each classified system, program, plan, or project as soon as practicable prior to the initial funding or implementation of the system, program, plan or project. Successive operating echelons shall prescribe such further detailed supplemental guides as may be deemed essential to assure accurate and consistent classification. In preparing classification guides, originators should review reference (ah), DoD 5200.1-H, "DoD Handbook for Writing Security Classification Guidance."

b. Classification guides shall:

1. Identify the information elements to be protected, using categorization to the extent necessary to ensure that the information involved can be identified readily and uniformly;

2. State which of the classification designations (i.e., Top Secret, Secret, or Confidential) applies to the information;

3. State the duration of classification in terms of a period of time or future event. When such duration is to exceed six years, the reason for such extension shall be provided in the guide. However, if the inclusion of classified reasons would result in a level of classification for a guide that would inhibit its desirable and required dissemination, those reasons need be recorded only on or with the record copy of the guide (see paragraph 2-301c); and

4. Either specifically indicate that the designations, time limits, markings, and other requirements of Executive Order 12065 are to be applied to information classified pursuant to the guide in accordance with DoD 5200.1-R or specify how they are to be applied.

c. Each classification guide shall be approved personally and in writing by an official with original Top Secret classification authority whose identity shall appear on the guide. Such approval constitutes an original classification decision.

2-401 Multiservice Interest

For each classified system, program, project, plan or item involving more than one Component of the Department of Defense, a classification guide shall be issued by: (i) the element in the Office of the Secretary of Defense that assumes or is expressly designated to exercise overall cognizance over it; or (ii) the Department of Defense Component that is expressly designated to serve as the executive or administrative agent for the particular effort.

2-402 Other Multiservice Interest Cases

The Deputy Under Secretary of Defense (Policy) shall develop, in coordination with the designated senior official (paragraphs 13-301 and 13-302) of each interested Department of Defense Component, and issue appropriate classification guides covering general subject matters that will be involved in individual systems or equipments and for which it is deemed essential to establish proper bases for uniform, consistent classification assignments.

2-403 Research, Development, Test and Evaluation

A program security classification guide shall be developed for each system and equipment development program that involves research, development, test and evaluation (RDT&E) of technical information. For each such program covered by an approved Decision Coordinating Paper (DCP) or Program Memorandum (PM), initial basic classification guidance applicable to technical characteristics of the system or equipment shall be developed and submitted with the proposed DCP or PM to the Under Secretary of Defense for Research and Engineering for approval. A detailed classification guide shall be developed and issued as near in time as possible to the approval of the DCP or PM.

2-404 Project Phases

Whenever possible, classification guides shall cover specifically each phase of transition, i.e., research, development, test and evaluation, procurement, production, service use and obsolescence, with changes in assigned classifications to reflect the changing sensitivity of the information involved.

2-405 Review of Classification Guides

a. Classification guides shall be reviewed by the originator for currency and accuracy not less than once every two years. Changes shall issued promptly. If no changes are made, the originator shall so annotate the record copy and show the date of the review.

b. Classification guides issued prior to 1 December 1978 that are in current use must be updated to meet the requirements of paragraph 2-400 in accordance with pertinent provisions of this Regulation. Such updating should be completed prior to December 1, 1978. Converting previous declassification determinations directed by classification guides shall be accomplished in accordance with the following:

1. Classifications subject to the General Declassification Schedule of Executive Order 11652: The date for declassification shall be restated as a finite date.

2. Classifications exempt from the General Declassification Schedule of Executive Order 11652:

(a) A date for declassification at the end of any period not in excess of twenty years from the date of original classification may be carried forward but shall be restated as a finite date, i.e., day, month and year.

(b) A date for declassification in excess of twenty years from the date of original classification or an indeterminate date or event for declassification may not be carried forward but shall be converted to a finite date for declassification or for review for declassification not more than twenty years from the date of original classification.

(c) In any case where a classification guide provides for the classification of foreign government information as defined herein, a date for declassification review shall be set at thirty years from the date of origin, acquisition or classification of the information by the United States, whichever is earlier.

2-406 Distribution of Classification Guides

a. A copy of each approved classification guide and changes thereto other than those covering Sensitive Compartmented Information (SCI) shall be sent to the Director of Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) and to the Director of Information Security, Office of the Deputy Under Secretary of Defense (Policy). A copy of each approved classification guide covering SCI shall be submitted to and maintained by the Senior Intelligence Officer who has security cognizance over the issuing activity.

b. Two copies of each approved classification guide and changes thereto shall be sent by the originator to the Administrator, Defense Documentation Center (DDC), Defense Logistics Agency unless such guide is classified Top Secret, or covers Sensitive Compartmented Information, or is determined by the approver of the guide to be too sensitive for automatic distribution to DoD Components. Each classification guide forwarded to DDC must bear one of the following distribution limitation statements on its front cover or first page if there is no cover:

1. "U.S. Gov't and its contractors."
2. "U.S. Gov't only."
3. "DoD and DoD contractors only."
4. "DoD only."

2-407 Index of Security Classification Guides

a. All security classification guides, except as provided in subparagraph b., below, issued pursuant to the provisions of this Regulation shall be listed in the "DoD Index of Security Classification Guides," DoD 5200.1-I (reference (ao)), on the basis of information provided on

DD Form 2024, "DoD Security Classification Guide Data Elements." The originator of each guide shall execute DD Form 2024 when the guide is approved, changed, revised, reissued, cancelled and when its biennial review is accomplished. The original copy of each executed DD Form 2024 will be forwarded to the Office of the Deputy Under Secretary of Defense (Policy) which will maintain the Index. Report Control Symbol DD-Comp (A & AR) 1418 applies to this information collection system.

b. Any classification guide that, because of classification considerations, is not listed in accordance with subparagraph a., above, shall be reported by the originator to the Director of Information Security, Office of the Deputy Under Secretary of Defense (Policy). The report shall include the title of the guide, its date, and identification of the originating activity and original classification authority. A separate classified list of such guides will be maintained. Report Control Symbol DD-Comp (A & AR) 1418 applies to this information collection system.

Section 5

RESOLUTION OF CONFLICTS

2-500 General

When two or more offices, headquarters or activities disagree concerning a classification, declassification, or regrading action, the disagreement must be resolved promptly.

2-501 Procedures

If agreement cannot be reached by informal consultation, the matter shall be referred for decision to the lowest superior common to the disagreeing parties. If agreement cannot be reached at the major command (or equivalent) level, the matter shall be referred for decision to the headquarters office having overall classification management responsibilities for the Component. That office shall also be advised of any disagreement at any echelon if it appears that prompt resolution is not likely.

2-502 Final Decision

Disagreements between Department of Defense Component headquarters, if not resolved promptly, shall be referred for final resolution to the Office of the Deputy Under Secretary of Defense (Policy). If appropriate, that office may refer the question to the DoD Information Security Committee (paragraph 13-201) for action.

2-503 Timing

Action under this Section at each level of consideration shall be completed within thirty (30) days. Failure to reach a decision within thirty (30) days shall be cause for referral to the next level of consideration.

Section 6

OBTAINING CLASSIFICATION EVALUATIONS

2-600 Procedures

If a person not authorized to classify originates or develops information that he or she believes should be safeguarded, he or she shall:

- a. Safeguard the information in the manner prescribed for the intended classification;
- b. Mark the information (or cover sheet) with the intended classification designation prescribed in Section 5, Chapter I;
- c. Transmit the information under appropriate safeguards to an appropriate classification authority for evaluation. The transmittal shall state that the information is tentatively marked to protect it in transit. If such authority is not readily identifiable, the information should be forwarded to a headquarters activity of a Department of Defense Component, to the headquarters office having overall classification management responsibilities for a Department of Defense Component or to the Deputy Under Secretary of Defense (Policy). A determination whether to classify the information shall be made within 30 days of receipt;
- d. Upon decision by the classifying authority, the tentative marking shall be removed. If a classification is assigned, appropriate markings shall be applied; but
- e. In an emergency requiring immediate communication of the information, after taking the action prescribed by subparagraphs a. and b., above, transmit the information and then proceed in accordance with subparagraph c., above.

Section 7

INFORMATION DEVELOPED BY PRIVATE SOURCES

2-700 General

There are some circumstances in which information not meeting the definition in paragraph 1-303 may warrant protection in the interest of national security.

The Patent Secrecy Act of 1952 (35 U.S.C. 181-188) provides that the Secretary of Defense, among others, may determine that disclosure of an invention by granting of a patent would be detrimental to national security. See DoD Directive 5535.2, reference (w). A patent application on which a secrecy order has been imposed shall be handled as follows within the Department of Defense:

a. If the patent application contains information that warrants classification, it shall be assigned a classification and be marked and safeguarded accordingly. In addition, a cover sheet with wording as in 2-701b, below, shall be attached.

b. If the patent application does not contain information that warrants classification, the following procedures shall be followed:

1. A cover sheet (or cover letter for transmittal) shall be placed on the application with substantially the following language:

The attached material contains information on which secrecy orders have been issued by the United States Patent Office after determination that disclosure would be detrimental to national security (Patent Secrecy Act of 1952, 35 U.S.C. 181-188). Its transmission or revelation in any manner to an unauthorized person is prohibited by law. Handle as though classified: CONFIDENTIAL (or such other classification as would have been assigned had the patent application been within the definition provided in paragraph 1-303).

2. The information shall be withheld from public release; its dissemination within the Department of Defense shall be controlled; the applicant shall be instructed not to disclose it to any unauthorized person; and the patent application (or other document incorporating the protected information) shall be safeguarded in the manner prescribed for equivalent classified material.

c. If filing of a patent application with a foreign government is approved under provisions of the Patent Secrecy Act of 1952 and agreements on interchange of patent information for defense purposes, the copies of the patent application prepared for foreign registration (but only those copies) shall be marked at the bottom of each page as follows:

Withheld under the Patent Secrecy Act
of 1952 (35 U.S.C. 181-188).

Handle as: CONFIDENTIAL (or such other
level as has been determined).

2-702 Independent Research and Development

a. Information in a document or material that is a product of government-sponsored independent research and development conducted without access to classified information may not be classified unless the Government first acquires a proprietary interest in such product.

b. If no prior access was given but the person or company conducting the independent research or development believes that protection may be warranted in the interest of national security, the person or company should safeguard the information in accordance with paragraph 2-600 and submit it to an appropriate Department of Defense element for evaluation. The Department of Defense element receiving such a request for evaluation shall make or obtain a determination whether a classification would be assigned if it were government information. If the determination is negative, the originator shall be advised that the information is unclassified. If the determination is affirmative, the Department of Defense element shall make or obtain a determination whether a proprietary interest in the research and development will be acquired. If such an interest is acquired, the information shall be assigned proper classification. If no such interest is acquired, the originator shall be informed that there is no basis for classification and the tentative classification shall be cancelled.

2-703 Other Private Information

The procedure specified in paragraph 2-600 shall apply in any case not specified in paragraph 2-702, such as an unsolicited contract bid, in which private information is submitted to a Department of Defense element for a determination of classification.

Section 8

REGRADING

2-800 Raising to a Higher Level of Classification

The upgrading of classified information to a higher level than previously determined, by officials with appropriate classification authority and jurisdiction over the subject matter, is permitted only when all known holders of the information: (i) can be notified promptly of such action, and (ii) are authorized access to the higher level of classification or the information can be retrieved from those not authorized access to information at the contemplated higher level of classification.

2-801 Classification of Information Previously Determined to be
Unclassified

Unclassified information, once communicated as such, may be classified only when the classifying authority: (i) makes the determination required for upgrading in paragraph 2-800, (ii) determines that control of the information has not been lost by such communication and can still be prevented from being lost, and (iii) in the case of information released to secondary distribution centers, such as the Defense Documentation Center, determines that no secondary distribution has been made and can still be prevented.

2-802 Notification

All known holders of information that has been upgraded shall be notified promptly of the upgrading action.

2-803 Downgrading

When it will serve a useful purpose, original classification authorities may, at the time of original classification, specify that downgrading of the assigned classification will occur on a specified date or upon the occurrence of a stated event.

Section 9

INDUSTRIAL OPERATIONS

2-900 Classification in Industrial Operations

Classification of information in private industrial operations shall be based only on guidance furnished by the Government. Industrial management may not make original classification determinations and shall implement the classification decisions of the U.S. Government contracting authority.

2-901 Contract Security Classification Specification

DD Form 254, "Contract Security Classification Specification," shall be used to convey contractual security classification guidance to industrial management. DD Forms 254 shall be changed by the originator to reflect changes in classification guidance and reviewed for currency and accuracy not less than once every two years. Changes shall be in strict conformance with the provisions of this Regulation and references (aa) and (ab) and shall be provided to all holders of the DD Form 254 as soon as possible. When no changes are made as a result of the biennial review, the originator shall so notify all holders of the DD Form 254 in writing.

DECLASSIFICATION AND DOWNGRADING

Section 1

GENERAL PROVISIONS

3-100 Policy

Declassification of information shall be given emphasis comparable to that accorded classification. Information classified pursuant to Executive Order 12065 and prior orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of sensitivity of the information with the passage of time or on the occurrence of an event which permits declassification. When information is reviewed for declassification, pursuant to this Regulation or DoD Directive 5400.7, reference (q), information shall be declassified unless the declassification authority designated pursuant to paragraph 1-603, determines that the information continues to meet the classification requirements prescribed in paragraph 2-202 despite the passage of time.

3-101 Responsibility of Officials

Officials authorized, pursuant to paragraph 1-603, to declassify or downgrade information that is under the final classification jurisdiction of the Department of Defense shall take such action in accordance with the provisions of this Chapter.

3-102 Exceptional Cases

It is presumed that information that continues to meet the classification requirements of Section 2, Chapter II requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of that information and in such cases the information should be declassified. When such questions arise concerning Department of Defense information, they shall be referred to the Secretary of Defense, the Secretary of a Military Department, the senior departmental official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under Section 3 of this Chapter, an official with TOP SECRET classification authority, or in the case of classified Presidential information, to the Archivist of the United States. That official, after consultation with other agencies or Department of Defense Components having interest, shall determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure and, if so, declassify the information. (See also paragraph 11-200 with respect to foreign government information.)

If the Director of the Information Security Oversight Office, General Services Administration, determines that information is classified in violation of Executive Order 12065, the Director may require the activity that originally classified the information to declassify it. Any such decision by the Director may be appealed through the Director for Information Security, Office of the Deputy Under Secretary of Defense (Policy), to the National Security Council. The information shall remain classified until the appeal is decided or until one year from the date of the determination by the Director of the Information Security Oversight Office, whichever comes first.

Section 2

SYSTEMATIC REVIEW

3-200 General

a. The Secretary of Defense and the Secretaries of the Military Departments may prolong beyond twenty years classification of information over which they exercise classification jurisdiction utilizing the procedures outlined in paragraph 3-202 below. This authority may not be delegated. When classification is prolonged beyond twenty years, a date no more than ten years later shall be set for declassification or the next review. That date and the action specified shall be marked on the document. Subsequent reviews for declassification shall be set at no more than ten year intervals unless a longer interval has been authorized by the Director of the Information Security Oversight Office. Requests for such authorization shall be processed as prescribed in b., below.

b. A Department of Defense Component request for extension of the period between subsequent reviews for declassification of specific categories of documents or information shall be submitted to the Deputy Under Secretary of Defense (Policy) and shall include personal certification by the head of the Component that the classified information for which the waiver is sought was systematically reviewed as required, that a definitive date for declassification could not be determined, that results of the review established an identifiable need to retain classification for a period in excess of twenty additional years and a recommendation concerning the interval before the next required review is expected to be required or for automatic declassification.

c. The Secretary of Defense and the Secretaries of the Military Departments shall designate experienced personnel to assist the Archivist of the United States in the systematic review of twenty-year old U.S. originated information and thirty-year old foreign government information. (See paragraph 3-202d for procedures.) Such personnel

~11:

1. Provide guidance and assistance to National Archives employees in identifying and separating documents and specific categories of information within documents that are deemed to require continued classification;

2. Submit to the Secretary of Defense or Secretary of the appropriate Military Department recommendations for continued classification that identify documents or specific categories of information so separated; and

3. Refer doubtful cases to the DoD Component having classification jurisdiction over the information or material for resolution.

3-201 Systematic Review Guidelines

The Director of Information Security, Office of the Deputy Under Secretary of Defense (Policy) shall develop, in coordination with Department of Defense Components, guidelines for the systematic review for declassification of information under Department of Defense jurisdiction that has been classified twenty years or more. (See also Chapter XI, Foreign Government Information.) The Secretary of Defense, after consultation with the Archivist of the United States, shall promulgate these guidelines on or before May 29, 1979. The guidelines shall identify specific limited categories of information that, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond twenty years is needed. These guidelines are authorized for use by the Archivist of the United States and with the approval of the Secretary of Defense, by any agency having custody of the information covered by the guidelines. All information, except foreign government information (see Chapter XI), not identified in these guidelines as requiring review and for which a prior automatic declassification date has not been established shall be declassified automatically at the end of twenty years from the date of original classification. The guidelines shall be kept current. They shall be reviewed at least every other year and revised as necessary unless earlier review for revision is requested by the Archivist of the United States. Copies of the systematic review guidelines will be provided to the Information Security Oversight Office.

3-202 Systematic Review Procedures

- a. Except for foreign government information covered by Chapter XI, classified information constituting permanently valuable records of the Department of Defense, as defined by 44 U.S.C. 2103, and such information in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be systematically reviewed as it becomes twenty years old. Classified non-permanent records that are scheduled to be retained for more than twenty years need not be systematically reviewed but shall be reviewed for declassification upon

request. Transition to systematic review at twenty years shall be implemented as rapidly as possible and shall be completed by December 1, 1988.

b. Heads of Department of Defense Components shall, as early as possible but not later than February 1, 1979, direct that all security classified records twenty years old or older under DoD Component possession and control, including those held in Federal Records Centers or other storage areas, be surveyed to identify those that require scheduling for future disposition. Such scheduling must be accomplished by December 1, 1980.

c. All Department of Defense classified information transferred to the General Services Administration for accession into the Archives of the United States that is permanently valuable and more than twenty years old will be systematically reviewed for declassification by the Archivist of the United States with the assistance of the DoD personnel designated for the purpose pursuant to paragraph 3-200d. Such information shall be downgraded or declassified by the Archivist of the United States in accordance with Executive Order 12065, the directives of the Information Security Oversight Office, and DoD guidelines.

d. All twenty-year old Department of Defense classified information that is permanently valuable and in the possession or control of the Components of the Department of Defense, including that held in Federal Records Centers or other storage areas, shall be systematically reviewed for declassification by the DoD Component exercising control of such information. Systematic declassification review conducted by DoD Components and personnel designated pursuant to paragraph 3-200d shall proceed as follows:

1. Information over which the Department of Defense exercises exclusive or final original classification authority and, in accordance with the systematic review guidelines developed under paragraph 3-201, is to be declassified, shall be marked accordingly.

2. Information over which the Department of Defense exercises exclusive or final original classification authority and that has been recommended for continued protection by the responsible reviewer in accordance with the guidelines developed under paragraph 3-201 shall be identified by category by the reviewer and referred through established channels to the Secretary of Defense or the Secretary of a Military Department, as appropriate. These submissions shall:

- (a) Identify the information;

- (b) Recommend classification beyond twenty years to a specific future event certain to occur or for a specific period of time not to exceed ten years or, in the alternative, recommend a subsequent review date not more than ten years later; and

(c) State the reason for the recommended continued classification.

3. The Secretary of Defense or Secretary of the Military Department as appropriate shall determine personally and in writing which category(ies) of information shall remain classified and the dates for automatic declassification or subsequent review. The Archivist of the United States shall be notified in writing of this decision.

e. Classified information over which the Department of Defense does not exercise exclusive or final original classification authority may be declassified only in accordance with the systematic review guidelines, promulgated pursuant to reference (c), of the agency responsible for the classification. If such guidelines are not available or authorized for use by Department of Defense personnel, the information shall be referred to the responsible agency.

3-203 Systematic Review of Classified Cryptologic Information

Notwithstanding paragraphs 3-200, 3-201 and 3-202, the Director, National Security Agency shall develop recommendations for the establishment of special procedures for systematic review and declassification of classified cryptologic information that shall be consistent, so far as practicable, with the objectives of the above-cited paragraphs. These recommendations shall be submitted to the Secretary of Defense for review and approval. Prior to implementation, these procedures shall be reviewed and approved by the Director of the Information Security Oversight Office. Disapproval of these procedures by the Director of the Information Security Oversight Office may be appealed to the National Security Council. In such case, the procedures shall not be implemented until the appeal is decided.

Section 3

MANDATORY REVIEW

3-300 Information Covered

Upon request by a member of the public or a government employee or agency to declassify and release such information, any classified information shall be subject to review by the originating or responsible Department of Defense Component for declassification in accordance with this Section.

3-301 Presidential Information

a. Information ten or more years old originated by the President, the White House Staff, committees or commissions appointed by the President, or by others acting on behalf of the President, is, upon request, subject to mandatory review for declassification in accordance with procedures developed by the Archivist of the United States pursuant to reference (b).

b. Such information less than ten years old is exempt from the provisions of this Section.

3-302 Submission of Requests for Review

Requests for mandatory review of Department of Defense classified information shall be submitted as follows:

a. Requests shall be in writing and reasonably describe the information sought with sufficient particularity to enable the Component to identify documents containing that information and be reasonable in scope, e.g., does not involve such a large number or variety of documents as to leave uncertain the identity of the particular information sought.

b. Requests shall be submitted to the Office of the Assistant Secretary of Defense (Public Affairs), the Military Department, or other Component most concerned with the subject matter that is designated pursuant to Department of Defense Directive 5400.7 (reference (q)) to receive requests for records under the Freedom of Information Act. These offices are identified in appropriate Sections of Title 32 of the Code of Federal Regulations for each Department of Defense Component.

3-303 Requirements for Processing

Unless otherwise directed by the Assistant Secretary of Defense (Public Affairs) requests for mandatory review shall be processed as follows:

a. The designated office shall acknowledge receipt of the request. When a request does not satisfy the conditions of paragraph 3-302a, the requester shall be notified that unless additional information is provided or the scope of the request narrowed no further action will be undertaken.

b. Component action upon the initial request shall be completed within sixty days (forty-five working days). If no determination has been made within sixty days (forty-five working days) of receipt of the request, the requester shall be notified of his right to appeal and of the procedures for making such an appeal.

c. The designated office shall determine whether, under the declassification provisions of this Regulation, the requested information may be declassified, and, if so, make such information available to the requester, unless withholding is otherwise warranted under applicable law. If the information may not be released in whole or in part, the requester shall be given a brief statement as to the reasons for denial, notice of the right to appeal the determination within sixty days (forty-five working days) to a designated appellate authority (including name, title, and address of such authority), and the procedures for such an appeal.

d. When a request is received for information classified by another Department of Defense Component or an agency outside the Department of Defense, the designated office shall:

1. Forward the request to such Department of Defense Component or outside agency for review together with a copy of the document containing the information requested, where practicable, and where appropriate, with its recommendation to withhold any of the information;
2. Notify the requester of the referral unless the Component or outside agency to which the request is referred objects to such notice on grounds that its association with the information requires protection; and
3. Request, when appropriate, that the Component or outside agency notify the referring office of its determination.

e. If the request requires the rendering of services for which fees may be charged under Title 5 of the Independent Offices Appropriation Act, 31 U.S.C. 483a in accordance with reference (r), the Component may calculate the anticipated amount of fees to be charged and ascertain the requester's willingness to pay the allowable charges as a precondition to taking further action upon the request.

f. A requester may appeal to the head of a DoD Component or his designee whenever that DoD Component has not acted on an initial request within sixty days or the requester has been notified that requested information may not be released in whole or in part. Within thirty days after receipt, an appellate authority shall determine whether continued classification of the requested information is required in whole or in part, notify the requester of its determination, and make available to the requester any information determined to be releasable. If continued classification is required under the provisions of this Regulation, the requester shall be notified of the reasons therefor. If so requested, an appellate authority shall communicate its determination to any referring DoD Component or outside agency.

3-304 Foreign Government Information

Requests for mandatory review for the declassification of foreign government information shall be processed and acted upon in accordance with the provisions of this Section subject to the provisions of paragraph 11-202.

3-305 Prohibition

No Component in possession of a document shall in response to a request under the Freedom of Information Act or this Section refuse to confirm the existence or non-existence of the document, unless the fact

of its existence or non-existence would itself be classifiable under this Regulation.

Section 4

DECLASSIFICATION OF TRANSFERRED DOCUMENTS OR MATERIAL

3-400 Material Officially Transferred

In the case of classified information or material transferred pursuant to statute or Executive Order from one department or agency to another in conjunction with a transfer of functions (not merely for storage purposes), as distinguished from transfers merely for purposes of storage, the receiving department or agency shall be deemed to be the original classifying authority over such material for purposes of downgrading and declassification.

3-401 Material Not Officially Transferred

When any Component has in its possession classified information or material originated in an agency outside the Department of Defense that has ceased to exist and such information or material has not been transferred to another department or agency within the meaning of paragraph 3-400, or when it is impossible to identify the originating agency, the Department of Defense Component shall be deemed to be the originating agency for the purpose of declassifying or downgrading such information or material. If it appears probable that another department, agency, or Component may have a substantial interest in the classification of such information, the Component deemed to be the originating agency shall notify such other department, agency, or Component of the nature of the information or material and any intention to downgrade or declassify it. Until sixty days after such notification, the Component shall not declassify or downgrade such information or material without consulting the other department, agency, or Component. During such period, the other department, agency or Component may express objections to downgrading or declassifying such information or material.

3-402 Transfer for Storage or Retirement

Whenever practicable, classified documents shall be reviewed for downgrading or declassification before they are forwarded to a Records Center for storage or to the National Archives for permanent preservation. Any downgrading or declassification determination shall be indicated on each document by markings as required by Chapter IV.

Section 5

DOWNGRADING

3-500 Automatic Downgrading

Classified information marked for automatic downgrading is downgraded accordingly without notification to holders.

3-501 Downgrading Upon Reconsideration

Classified information not marked for automatic downgrading may be assigned a lower classification designation by the originator or by an official authorized to declassify the same information. (See paragraph 1-603.) Prompt notice of such downgrading shall be provided to known holders of the information.

Section 6

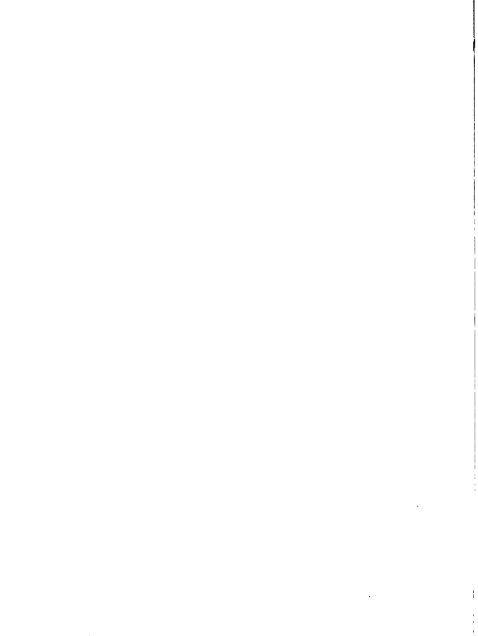
MISCELLANEOUS

3-600 Notification of Changes in Declassification

When classified material has been properly marked with specific dates or events for declassification it is not necessary to issue notices of declassification to any holders. However, when declassification action is taken earlier than originally scheduled, or the duration of classification is extended, the authority making such changes shall ensure prompt notification of all holders to whom the information was originally transmitted. The notification shall specify the marking action to be taken, the authority therefor and the effective date. Upon receipt of notification, recipients shall effect the proper changes and shall notify holders to whom they have transmitted the classified information. See paragraphs 4-400 and 4-404 for markings and the use of posted notices.

3-601 Foreign Relations Series

In order to permit the State Department editors of Foreign Relations of the United States to meet their mandated goal of publishing twenty years after the event, DoD Components shall assist the editors in the Department of State by facilitating access to appropriate classified materials in their custody and by expediting declassification review of items from their files selected for possible publication.



CHAPTER IV

MARKING

Section 1

GENERAL PROVISIONS

4-100 Designation

Subject to the exception in paragraph 4-102, information determined to require classification protection under the provisions of this Regulation shall be so designated. Designation by means other than physical marking may be used but shall be followed by physical marking as soon as possible.

4-101 Purpose of Designation

Designation by physical marking, notation, or other means serves to warn the holder about the classification of the information involved; to indicate the degree of protection against unauthorized disclosure that is required for that particular level of classification; and to facilitate downgrading and declassification actions.

4-102 Exception

No article which has appeared, in whole or in part, in newspapers, magazines or elsewhere in the public domain, or any copy thereof, that is being reviewed and evaluated to compare its content with classified information that is being safeguarded in the Department of Defense by security classification, may be marked with any security classification, control or other kind of restrictive marking. The results of the review and evaluation, if classified, shall be separate from the article in question.

4-103 Documents or Other Material in General

a. At the time of original classification, the following shall be shown on the face of paper copies of originally classified documents:

1. The identity of the original classification authority, unless he or she is the signer or approver of the document;
2. The date of classification and office of origin. The date and office of origin on a document at the time of its origination may be considered the date of classification and identification of the office of origin;

3. The overall classification of the document (see para 1-500);
4. The date or event for automatic declassification or for review for declassification;

5. Documents classified for more than six years shall also be marked with the identity by title of the TOP SECRET classification authority who authorized prolonged classification, unless that official also is the signer or approver, and annotated with the reasons the classification is expected to remain necessary despite the passage of time. The reasons may be stated by reference to the appropriate criteria listed in paragraph 2-301c; and

6. Any downgrading action to be taken and the date thereof.

b. At the time of origin, paper copies of derivatively classified documents shall show on their face:

1. The source of classification, i.e., a source document or classification guide. If classification is derived from more than one source, the phrase "multiple sources" will be shown and the identification of each source will be maintained with the file or record copy of the document;

2. The office of origin of the derivatively classified document;

3. The overall classification of the document (see paragraph 1-500);

4. The date or event for declassification or for review for declassification, carried forward from the classification source (see paragraph 4-402c). If the classification is derived from multiple sources, the latest date or event shall be shown; and

5. Any downgrading action to be taken and the date thereof.

c. In addition to the foregoing, paper copies of classified documents shall be marked as prescribed in Section 2 of this Chapter, in Chapter XI, if the document contains foreign government information, and with any applicable special notation listed in Section 5 of this Chapter. Such notations shall be carried forward from source documents to derivatively classified documents when appropriate.

d. To the extent practical, material other than paper copies of documents shall show the foregoing on the material itself or in related or accompanying documentation. (See paragraph 4-300.)

4-104 Identification of Classification Authority

a. Identification of a classification authority shall be shown on the "Classified by" line prescribed under paragraph 4-402 and shall be such that, standing alone, it is sufficient to identify a particular official, source document or classification guide.

1. If any information in a document or material is classified as an act of original classification, the classification authority who made the determination shall be identified on the "Classified by" line, unless the classifier is also the signer or approver of the document. (See paragraph 4-402.)

2. If the classification of all information in a document or material is derived from a single source (for example, a source document or classification guide), the "Classified by" line shall identify the source document or classification guide, including its date. (See paragraph 4-402.)

3. If the classification of information contained in a document or material is derived from more than one source document, classification guide, or combination thereof, the "Classified by" line shall be marked "multiple sources" and identification of all such sources shall be maintained with the file or record copy of the document. (See paragraph 4-402.)

4. If an official with requisite classification authority has been designated by the head of an activity to approve security classifications assigned to all information leaving the activity, the title of that designated official shall be shown on the "Classified by" line. The designated official shall maintain records adequate to support derivative classification actions. (See paragraph 4-402.)

b. Guidance concerning the identification of the classification authority on electronically transmitted messages is contained in paragraph 4-207.

4-105 Wholly Unclassified Material

Normally, unclassified material shall not be marked or stamped "Unclassified" unless it is essential to convey to a recipient of such material that it has been examined with a view to imposing a security classification and that it has been determined that it does not require classification.

SPECIFIC MARKINGS ON DOCUMENTS

4-200 Overall and Page Marking

Except as otherwise specified for working papers (see paragraph 7-304), the overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked, stamped or affixed permanently at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Each interior page shall be marked top and bottom according to its content. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page when such marking is necessary to achieve production efficiency and the particular information to which classification is assigned is otherwise sufficiently identified consistent with the intent of paragraph 4-202. In any case, the classification marking of a page shall not supersede the classification marking of portions (paragraph 4-202) of the page marked with lower levels of classification.

4-201 Marking Components

The major components of some complex documents are likely to be used separately. In such instances, each major component shall be marked as a separate document in accordance with Section 1 of this Chapter. Examples include: (i) each annex, appendix, or similar component of a plan, program or operations order; (ii) attachments and appendices to a memorandum or letter; (iii) each major part of a report.

4-202 Portion Marking

a. Each section, part, paragraph, subparagraph, or similar portion of a classified document shall be marked to show the level of classification of the information contained in or revealed by it, or that it is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contains or reveals classified information. Classification levels of portions of a document, except as provided in paragraph 4-204, shall be shown by the appropriate classification symbol placed immediately following the portion letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. In marking sections, parts, paragraphs, subparagraphs, or similar portions, the parenthetical symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for unclassified, shall be used. When appropriate, the symbols "RD" for Restricted Data and "FRD" for Formerly Restricted Data shall be added, e.g., "(S-RD)" or "(C-FRD)." In addition, portions that contain Critical Nuclear Weapon Design Information (CNWDI) will be so marked "(N)" following the classification, e.g., "(S-RD)(N)." To illustrate the foregoing, if a lead-in paragraph is unclassified and a subparagraph is Secret-Restricted Data-Critical Nuclear Weapon Design Information, the markings will be:

- "1. (U) This is the unclassified lead-in paragraph.
a. (S-RD)(N) This is the classified subparagraph."

b. Portion marking of Department of Defense documents containing foreign government information shall be in accordance with paragraph 11-304.

c. Illustrations, photographs, figures, graphs, drawings, charts and similar portions of classified documents will be clearly marked to show their classification or unclassified status. Such markings shall not be abbreviated and shall be prominent and placed within or contiguous to the portion. Captions of such portions shall be marked on the basis of their content alone by placing the symbol "(TS)," "(S)," "(C)," or "(U)" immediately preceding the caption.

d. If, in an exceptional situation, parenthetical portion marking is determined to be impracticable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification. Thus, for example, each portion of a classified document need not be separately marked if all portions are classified at the same level provided a statement to that effect is included in the document.

e. When elements of information in one portion require different classifications, but segregation into separate portions would destroy continuity or context, the highest classification required for any item shall be applied to that portion or paragraph.

f. The Director of the Information Security Oversight Office may, for good cause, grant and revoke waivers of the foregoing portion marking requirements. A request by a DoD Component for a waiver of portion marking requirements shall be submitted to the Deputy Under Secretary of Defense (Policy) and include the following: (i) identification of the information or class of documents for which such waiver is sought; (ii) detailed explanation of why the waiver should be granted; (iii) the Component's judgment as to the anticipated dissemination of the information or class of documents for which the waiver is sought and (iv) the extent to which such information subject to the waiver may be a basis for derivative classification.

4-203 Compilations

Where classification is required to protect a compilation of information under paragraph 2-211, the overall classification assigned to such documents shall be placed conspicuously at the top and bottom of each page and on the outside of the front and back covers, if any, and an explanation of the basis for the assigned classification shall be included on the document or in its text.

4-204 Subjects and Titles of Documents

Classified subjects or titles of documents shall be marked with the appropriate symbol, "(TS)", "(S)", "(C)", or "(U)" placed immediately following and to the right of the item. When applicable, other appropriate symbols, e.g., "(RD)" and "(FRD)", shall be added.

4-205 File, Folder, or Group of Documents

Files, folders or groups of documents shall be marked conspicuously according to the highest classification of any classified document included therein. Classified document cover sheets may be used for this purpose.

4-206 Transmittal Documents

A transmittal document, including endorsements and comments when such endorsements and comments are added to the basic communication, shall carry on its face a prominent notation as to the highest classification of the information transmitted by it, and a legend showing the classification, if any, of the transmittal document, endorsement or comment standing alone. For example, an unclassified document that transmits as an attachment a classified document shall bear a notation substantially as follows: "UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURE."

4-207 Electronically Transmitted Messages

a. The copy of a classified message (e.g., DD Form 173, Joint Messageform) approved for transmission and maintained as the record copy shall be marked as required by paragraph 4-103 for other documents.

b. The first item of information in the text of a classified electronically transmitted message shall be its overall classification. Paper copies of classified electronically transmitted messages shall be marked at the top and bottom with the assigned classification. Portions shall be marked as prescribed herein for paper copies of documents. When such messages are printed by an automated system, classification markings may be applied by that system, provided that the markings so applied are clearly distinguishable on the face of the document from the printed text.

c. The originator of a classified electronically transmitted message shall be considered the accountable classifier under paragraph 2-100. The highest level official identified on the message as the sender thereof or, in the absence of such identification, the head of the organization originating the message, is deemed to be the classifier of the message and, with respect to any such messages classified more than six years, is deemed to be the official who authorized the prolonged classification. Thus, "classified by" and "extended by" lines are not required on such messages. The originator is responsible for maintaining

adequate records as required by paragraph 4-103b to show the source of an assigned derivative classification and, in the case of an original classification prolonged more than six years, the reason and extension authority.

d. The last line of text of a classified electronically transmitted message shall show the date for automatic declassification or for review for declassification and, for any such message originally classified for more than six years, the reason for prolonged classification, by abbreviated markings from paragraph 4-402.

e. Any document, the classification of which is based solely upon the classification of the content of a classified electronically transmitted message, shall cite the message on the "classified by" line of the newly created document.

f. Reference (c) provides that with respect to electronically transmitted messages, a single line of abbreviations or codes may be utilized to satisfy most of the marking requirements of this Chapter provided that the full text represented by each such abbreviation or code and its relation to each pertinent paragraph of this Chapter is readily available to each expected user of the classified messages involved. The use of such codes or abbreviations by DoD Components, however, is prohibited, unless approved by the Deputy Under Secretary of Defense (Policy) or authorized by an amendment to this Regulation.

4-208 Translations

Translations of United States classified information into a language other than English shall be marked to show the United States as the country of origin, with the appropriate U.S. classification markings and the foreign language equivalent thereof. (See Appendix A.)

Section 3

MARKINGS ON SPECIAL CATEGORIES OF MATERIAL

4-300 General Provisions

Security classification and declassification instructions assigned by the classifier shall be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal or similar device, on classified material other than paper copies of documents, and on containers of such material, if possible. If marking the material or container is not practicable, written notification of the security classification and declassification instructions shall be furnished to recipients. The following procedures for marking various kinds of material containing classified information are not all inclusive and may be varied to accommodate the physical characteristics of the material containing the classified information and with organizational and operational requirements.

4-301 Charts, Maps and Drawings

Charts, maps and drawings shall bear the appropriate classification marking under the legend, title block or scale, in a manner that differentiates between the overall classification of the document and the classification of the legend or title itself. The higher of these markings shall be inscribed at the top and bottom of each such document. When folding or rolling charts, maps or drawings would cover the classification markings, additional markings shall be applied that are clearly visible when the document is folded or rolled.

4-302 Photographs, Films and Recordings

Photographs, films (including negatives), recordings, and their containers shall be marked in such a manner as to assure that a recipient or viewer will know that classified information of a specified level of classification is involved.

a. Photographs. Negatives and positives shall be marked, whenever practicable, with the appropriate classification designation. Roll negatives or positives may be so marked at the beginning and end of each strip. Negatives and positives shall be kept in containers bearing conspicuous classification markings. When self-processing film or paper is used to photograph or reproduce classified information, all parts of the last exposure shall be removed from the camera and destroyed as classified waste, or the camera shall be protected as classified. All prints and reproductions shall be conspicuously marked with the appropriate classification designation and downgrading (if applicable) and declassification instructions on the face side of the print if possible. Where such markings cannot be applied to the face side, they may be stamped on the reverse side or affixed by pressure tape label, stapled strip or other comparable means.

b. Transparencies and Slides. Applicable classification markings shall be shown clearly on the image of each transparency or slide, if possible, or on its border, holder, or frame. Other applicable markings shall be shown on the border, holder, or frame.

c. Motion Picture Films. Classified motion picture films and video tapes shall be marked at the beginning and end of each reel by titles bearing the appropriate classification. Such markings shall be visible when projected. Reels shall be kept in containers bearing conspicuous classification, declassification and, if applicable, downgrading markings.

d. Recordings. Sound, magnetic or electronic recordings shall contain at the beginning and end a clear statement of the assigned classification that will provide adequate assurance that any listener or receiver will know that classified information of a specified level is involved. Recordings shall be kept in containers or on reels that bear conspicuous classification, declassification and, if applicable, downgrading markings.

e. Microforms. Microforms are images, usually produced photographically on transparent or opaque materials, in sizes too small to be read by the unaided eye. Accordingly, the assigned security classification and abbreviated downgrading (if applicable) and declassification instructions (see paragraph 4-402) shall be conspicuously marked on the microform medium or its container, so as to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. Further marking and handling shall be as appropriate for the particular microform involved. For example, roll film microforms (or roll microfilm employing 16, 35, 70, or 105 mm films) may generally be handled as provided for roll motion picture film in paragraph 4-302c and decks of "aperture cards" may be handled as provided in paragraph 4-303 for decks of accounting machine punched cards. Whenever possible, microfiche, microfilm strips and microform chips shall be handled in accordance with this paragraph.

4-303 Decks of Accounting Machine Punched Cards

A deck of classified accounting machine punched cards may be considered as a single document. Only the first and last card require classification markings. An additional card shall be added (or the job control card modified) to identify the contents of the deck (at a minimum, the number of cards) and the highest classification therein. Alternatively, a manual log for decks undergoing frequent changes may be employed. Cards removed for separate processing or use and not immediately returned to the deck shall be protected to prevent compromise of any classified information contained therein, and for this purpose shall be marked individually as prescribed in paragraph 4-200.

4-304 Removable Automatic Data Processing and Word Processing Storage Media

Removable information storage media, employed with automatic data processing (ADP) systems and typewriters or word processing systems, shall bear external markings and internal notations sufficient to assure that any recipient of the media, or of the classified information contained therein when reproduced by any means, will know that classified information of a specific classification level is involved. This category media and devices that store digitally recorded information are generally intended to be mounted or removed by the users or operators. Examples include magnetic tape reels, cartridges and cassettes; removable discs, disc cartridges, disc packs and diskettes; paper tape reels; and magnetic cards. (Requirements for the security of non-removable ADP storage media and clearance or declassification procedures for various ADP storage media are contained in reference (am)).

4-305 Documents Produced by ADP Equipment

At a minimum, the first page, and the front and back covers, if any, of documents produced by ADP equipment shall be marked as prescribed in paragraph 4-200. Classification markings of interior pages may be applied by the ADP equipment or by other means. When the application of declassification instructions and other markings prescribed by paragraph 4-103 by the ADP equipment is not consistent with economic and efficient use of such equipment, such instructions and markings may be applied to a document produced by ADP equipment by superimposing upon the first page of such document a "Notice of Declassification Instructions and Other Associated Markings." Such Notice shall include the date or event for declassification or review for declassification and all other such applicable markings. If individual pages of a document produced by ADP equipment are removed or reproduced for distribution to other users, each such page or group of pages shall be marked as prescribed in paragraph 4-103 or by superimposing on each such page or group of pages, a copy of any "Notice of Declassification Instructions and Other Associated Markings" applicable to such page or group of pages.

4-306 Material for Training Purposes

In utilizing unclassified documents or material to simulate classified documents or material for training purposes, such documents or material shall be marked "(insert classification designation) for training, otherwise unclassified."

4-307 Miscellaneous Material

Documents and material such as rejected copy, typewriter ribbons, carbons, and similar items developed in connection with the handling, processing, production, and utilization of classified information shall be handled in a manner that assures adequate protection of the classified information involved and destruction at the earliest practicable moment (see Section 2, Chapter V). Unless a requirement exists to retain this type of material or documents for a specific purpose, there is no need to mark, stamp, or otherwise indicate that the information is classified.

4-308 Special Access Program Documents and Material

Additional markings as prescribed in directives, regulations and instructions relating to an approved special access program shall be applied to documents and material containing information subject to the special access program. Such additional markings shall not serve as the sole basis for continuing classification of the documents or material to which the markings have been applied. When appropriate, such markings shall be excised to facilitate timely declassification, downgrading or removal of the information from special control procedures.

Other markings required for documents by paragraph 4-103 shall be accomplished as prescribed in this Section for the security classification and declassification instructions assigned by the classifier or in any other appropriate manner, where practicable.

Section 4

CLASSIFICATION AUTHORITY, DURATION AND CHANGE MARKINGS

4-400 Declassification and Regrading Marking Procedures

Whenever classified information is downgraded or declassified earlier than originally scheduled, or upgraded, the material shall be marked promptly and conspicuously to indicate the change, the authority for the action, the date of the action and the identity of the person taking the action. In addition, except for upgrading (see paragraph 4-403), prior classification markings shall be canceled, if practicable, but in any event those on the first page, and the new classification markings, if any, shall be substituted. In cases where classified information is downgraded or declassified in accordance with the downgrading and declassification markings prescribed in paragraph 4-402, such markings shall be a sufficient notation of the authority for such action.

4-401 Applying Derivative Declassification Dates

a. New material that derives its classification from information classified on or after December 1, 1978 shall be marked with the declassification date, event, or date for review assigned to the source information.

b. New material that derives its classification from information classified prior to December 1, 1978, shall be treated as follows:

1. If the source material bears a declassification date or event not more than 20 years from the date of origin, the date or event shall be carried forward to the new material;

2. If the source material bears no declassification date or event, or bears an indeterminate date or event such as "Upon Notification by Originator," "Cannot Be Determined," "Impossible to Determine," etc., or is marked for declassification beyond 20 years from date of origin, the new material shall be marked with a date for review for declassification at 20 years from the date of original classification of the source material; and

3. If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond 30 years from date of origin, the new material shall be marked for review for declassification at 30 years from the time the

information was originated by the foreign government or international organization of governments, or acquired or classified by the DoD, whichever is earlier.

c. New material that derives its classification from a classification guide issued prior to December 1, 1978 that has not been updated to conform with this Regulation shall be treated as follows:

1. If the guide specifies a declassification date or event 20 years or less from the date of original classification, that date or event shall be applied to the new material.

2. If the guide specifies a declassification date or event more than 20 years from the date of original classification, or no declassification date or event, or an indeterminate date or event as in subparagraph b.2 above, a date for review for declassification at 20 years from the date of original classification shall be applied to the new material.

PARAGRAPH 4-402, "COMMONLY USED
MARKINGS," FOLLOWS ON NEXT TWO PAGES

4-402 Commonly Used Markings

At the time of origin, each classified document is marked on its face with one or more standard markings as follows:

a. Original Classification Not to Continue More than Six Years: The following markings are used with an original classification that will not continue beyond six years (paragraph 4-103a):

Classified by _____ (See Note 1)
Declassify on _____ (See Note 2)
Message Abbreviation:
DECL _____ (See Note 3)

b. Original Classification to Continue More than Six Years but Not in Excess of 20 Years. The following markings are used with an original classification that will continue beyond six years but not in excess of 20 years (paragraph 4-103a):

Classified by _____ (See Note 1)
OR Declassify on _____ (See Note 4.a.)
Review on _____ (See Note 4.b.)
Extended by _____ (See Note 5)
Reason _____ (See Note 6.a.)
Message Abbreviations:
DECL _____ (See Note 3)
OR REVW _____ (See Note 7)
REAS _____ (See Note 8.b.)

c. Derivative Classification. The following markings are used with a derivative classification (paragraph 4-103b):

Classified by _____ (See Note 8)
OR Declassify on _____ (See Note 9.a.)
Review on _____ (See Note 9.b.)
Message Abbreviations:
DECL _____ (See Note 3)
OR REVW _____ (See Note 7)

d. Downgrading. The following marking is used to specify a downgrading (paragraph 4-103a and b):

Downgrade to _____ on _____ (See Note 10)
Message Abbreviation:
DG/ / _____ (See Note 11)

e. The Restricted Data and Formerly Restricted Data markings (paragraphs 4-501 and 4-502) are, in themselves, evidence of extended classification. Therefore, except for electronically transmitted messages, only a completed "classified by" line is added above such marking.

4-402 Notes

Note 1: Insert identification of original classification authority. This line may be omitted if the original classification authority is also the signer or approver of the document.

Note 2: Insert the specific date or an event certain to occur.

Note 3: Insert day, month and year for declassification, e.g., "6 Jun 79" or an event certain to occur.

Note 4: Insert: a. The specific date or an event certain to occur;

b. The date for declassification review.

Note 5: Insert identification of original Top Secret classification authority. This line may be omitted if the authority is the signer or approver of the document.

Note 6: Insert: a. The paragraph citation 2-301.c. and the number (1 thru 8) that identifies the applicable reason for the extended period of classification, e.g., "2-301.c.7" or "2-301.c.3 and 5;"

b. Only the number (1 thru 8) that identifies the applicable reason, e.g., "7" or "3 & 5."

Note 7: Insert day, month, and year for declassification review, e.g., "6 Jun 89."

Note 8: Insert identity of the single security classification guide, source document, or other authority for the classification. If more than one such source is applicable, insert the words "multiple sources."

Note 9: Insert: a. The specific date or event for declassification (when multiple sources are used, the latest of the declassification dates applicable to any of the source material is applied to the new document);

b. The date for declassification review, as indicated by the source security classification guide or other source document as appropriate (when multiple sources are used, the latest of the declassification review dates applicable to any of the source material is applied to the new document).

Note 10: Insert Secret or Confidential and specific date or event, e.g., "Downgrade to CONFIDENTIAL on 6 July 1983."

Note 11: Insert "S" or "C" to indicate the downgraded classification and specific date or event, e.g., "DG/C/6 Jun 83."

4-403 Upgrading

When material is upgraded it shall be promptly and conspicuously marked as prescribed in paragraph 4-400 except that in all such cases the old classification markings shall be cancelled and new substituted therefor.

4-404 Limited Use of Posted Notice for Large Quantities of Material

a. When the volume of material is such that prompt remarking of each classified item cannot be accomplished without unduly interfering with operations, the custodian may attach downgrading and declassification notices to the storage unit in lieu of the remarking required by paragraph 4-400. Each notice shall specify the authority for the downgrading or declassification action, the date of the action, and the storage unit to which it applies.

b. When individual documents or materials are permanently withdrawn from storage units, they shall be remarked promptly as prescribed by paragraph 4-400. However, when documents or materials subject to a downgrading or declassification notice are withdrawn from one storage unit solely for transfer to another, or a storage unit containing such documents or materials is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

Section 5

ADDITIONAL WARNING NOTICES

4-500 General Provisions

a. In addition to the marking requirements prescribed in paragraph 4-103, the warning notices prescribed in this Section shall be prominently displayed on classified documents or materials, when applicable. In the case of documents, these warning notices shall be marked conspicuously on the outside of the front cover, or on the first page if there is no front cover.

b. When display of warning notices on other materials is not possible, their applicability to the information shall be included in the written notification of the assigned classification.

c. Stamps in current use for application of warning notices previously authorized for RESTRICTED DATA, FORMERLY RESTRICTED DATA, and INTELLIGENCE SOURCES AND METHODS may be used until repurchase becomes necessary or until May 31, 1979, whichever is earlier.

4-501 Restricted Data

Classified documents or material containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended, shall be marked as follows:

"RESTRICTED DATA"

"This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions."

4-502 Formerly Restricted Data

Classified documents or material containing Formerly Restricted Data, as defined in Section 142.d, Atomic Energy Act of 1954, as amended, but no Restricted Data, shall be marked as follows:

"FORMERLY RESTRICTED DATA"

"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954."

4-503 Intelligence Sources and Methods Information

Classified information or material involving intelligence sources and methods and subject to specific dissemination controls established in reference (m), shall be marked with the following additional warning notice:

"WARNING NOTICE--Intelligence Sources
and Methods Involved."

4-504 COMSEC Material

COMSEC documents, prior to release to contractors, will contain on the title page, or first page if no title page exists, the following notation:

"COMSEC Material - Access by Contractor Personnel Restricted
to U.S. Citizens Holding Final Government Clearance."

This notation shall be placed on COMSEC documents or material at the time of their origination when release to contractors can be anticipated. Other COMSEC documents or material shall be marked in accordance with National COMSEC Instruction (NACSI) 4005 (reference (ae)). Foreign dissemination of COMSEC information is governed by National Communications Security Committee (NCSC) Policy Directive 14-2 (reference (an)).

4-505 Dissemination and Reproduction Notice

Classified information that is determined by a DoD originator to be subject to special dissemination or reproduction limitations, or both, shall include, as applicable, a statement or statements on its cover sheet, first page or in the text, substantially as follows:

"Reproduction requires approval of originator or higher DoD authority."

"Further dissemination only as directed by (Insert appropriate office or official) or higher DoD authority."

4-506 Other Notations

Other notations of restrictions on reproduction, dissemination or extraction of classified information may be used as authorized by references (e), (m), (n), (o), (p), (t), and (v).

Section 6

REMARKING OLD MATERIAL

4-600 General

Documents and material already marked under Executive Order 11652, as amended, or predecessor Orders and directives shall be remarked in conformity with this Chapter when (i) information extracted from material so marked is to be conveyed or (ii) the document or material itself is to be disseminated in any manner, or (iii) the document or material is reviewed for specific purposes under Chapter III. When such document or material is withdrawn temporarily from files or storage merely for reference purposes, transfer to other files, or storage within the same activity it need not be remarked. Whenever remarking of such documents or material is required, it shall be accomplished in accordance with this Section.

4-601 Foreign Government Information

Documents or material classified before December 1, 1978 that contain foreign government information shall be marked for review for declassification 30 years from the date of origin, e.g., "Review on (insert date)."

4-602 Remarking Documents or Material Marked "Subject to the General Declassification Schedule" or "Advanced Declassification Schedule"

A document or material, classified prior to December 1, 1978 and marked for automatic declassification in accordance with the General Declassification Schedule (GDS) or an Advanced Declassification Schedule

(ADS) under Executive Order 11652 need not be remarked. However, should a determination be made under Section 3, Chapter 11 to extend classification beyond the declassification date or event specified by the GDS or an ADS, the document or material shall be remarked in accordance with paragraph 4-402b. Such extension may be made only in accordance with paragraph 1-600.

4-603 **Marking Documents or Material Marked as "Exempt from the GDS" or Not Marked With Any Declassification Instructions**

A document or material classified before December 1, 1978 and marked as exempt from the GDS under Executive Order 11652 with a date or event for declassification 20 years or less from the date of origin, shall not be remarked. However, if a document or material exempted from the GDS is marked with a declassification date in excess of 20 years from the date of origin or does not bear a specific declassification date or event, it shall be marked with a date for review for declassification at 20 years from the date of origin of the document, e.g., "Review on (insert date)."

4-604 **Marking Documents or Material Marked "Group 4"**

a. Information classified under Executive Order 10501, as amended, that is contained in a document or material marked as Group 4 and still so marked, was placed by Executive Order 11652 under the General Declassification Schedule and subject to automatic declassification thereunder as follows:

1. All such information originally classified as Top Secret becomes declassified on December 31 of the tenth year from the year of origin or December 31, 1982, whichever is earlier;

2. All such information originally classified as Secret becomes declassified on December 31 of the eighth year from the year of origin or December 31, 1980, whichever is earlier; and

3. All such information originally classified as Confidential becomes declassified on December 31 of the sixth year from the year of origin or December 31, 1978, whichever is earlier.

b. When such information is determined to have been automatically declassified under subparagraph a. 1., 2., or 3., above, remarking of a document or material is not necessary but old classification markings shall be canceled on at least the first page. In cases where such information remains classified under subparagraph a. 1., 2., or 3., a finite date for declassification shall be shown on a "declassify on" line, prior classification markings canceled on at least the first page, and current classification designations substituted therefor. However, should a determination be made under Section 3, Chapter 11 to extend classification beyond the declassification date or event specified by

the GDS, the document or material shall be remarked in accordance with paragraph 4-402b. Such extension may be made only in accordance with paragraph 1-600.

4-605 Remarking Documents or Material Marked Group 1, 2 or 3, or Not Group Marked

Information classified before June 1, 1972 that is contained in a document or material marked as Group 1, 2 or 3 under Executive Order 10501 as amended, or not group marked, shall be remarked to show a date for review for declassification 20 years from the date of origin, e.g., "Review on (insert date)."

4-606 Earlier Declassification

Nothing in this Section shall be construed to preclude declassification under paragraph 3-100.

CHAPTER V

SAFEKEEPING AND STORAGE

Section 1

STORAGE AND STORAGE EQUIPMENT

5-100 General Policy

Classified information shall be stored only under conditions adequate to prevent unauthorized persons from gaining access. The requirements specified in this Regulation represent the minimum acceptable security standards. DoD policy concerning the use of force for the protection of property or information is specified in reference (ac).

5-101 Standards for Storage Equipment

The General Services Administration (GSA) establishes and publishes minimum standards, specifications and supply schedules for containers, vaults, alarm systems and associated security devices suitable for the storage and protection of classified information. Heads of DoD Components may establish additional supplementary controls to prevent unauthorized access. Security filing cabinets conforming to Federal specifications bear a Test Certification Label on the locking drawer attesting to the security capabilities of the container and lock (on some early cabinets, the label was located on the wall inside the locked drawer compartment). Such cabinets manufactured after February 1962 will also be marked "General Services Administration Approved Security Container" on the outside of the top drawer.

5-102 Storage of Classified Information

Whenever classified information is not under the personal control and observation of an authorized person, it will be guarded or stored in a locked security container as prescribed below:

a. Top Secret. Top Secret information shall be stored in:

1. A safe-type steel file container having a built-in, three-position, dial-type combination lock approved by the General Services Administration, or a Class A vault or vault type room that meets the standards established by the head of the DoD Component; or

2. An alarmed area, provided such facilities are adjudged by the local responsible official to afford protection equal to or better than that prescribed in 1. above. When an alarmed area is utilized for the storage of Top Secret material, the physical barrier must be adequate to prevent (a) surreptitious removal of the material, and (b) observation

when observation would result in the compromise of the material. The physical barrier must be such that forcible attack will give evidence of attempted entry into the area or room. The alarm system must as a minimum provide immediate notice to a security force of attempted entry.

b. Secret and Confidential. Secret and Confidential information shall be stored in the manner prescribed for Top Secret; or in a Class 1 vault, or a vault-type room, strong room, or secure storage room, that meets the standards prescribed by the head of the DoD Component; or, until phased out, in a steel filing cabinet having a built-in, three-position, dial type combination lock; or, as a last resort, an existing steel filing cabinet equipped with a steel lock bar, provided it is secured by a GSA approved changeable combination padlock.

c. Specialized Security Equipment.

1. Field Safe and One-drawer Container. One-drawer field safes, and GSA approved security containers are used primarily for storage of classified information in the field and in transportable assemblages. Such containers must be securely fastened or guarded to prevent the theft of the container.

2. Map and Plan File. A GSA approved Map and Plan file has been developed for storage of odd-sized items such as computer cards, maps, and charts.

d. Other Storage Requirements. Storage areas for bulky material containing classified information shall have access openings secured by GSA-approved changeable combination padlocks (Federal specification FF-PlIF series) or key-operated padlocks with high security cylinders (exposed shackle, Military specification P-43951 series, or shrouded shackle, Military specification P-43607 series).

1. When combination padlocks are used, the provisions of paragraph 5-104 apply.

2. When key-operated high security padlocks are used, keys shall be controlled as classified information with classification equal to the classification of the information being protected and:

(a) A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks;

(b) A key and lock control register shall be maintained to identify keys for each lock and their current location and custody;

(c) Keys and locks shall be audited each month;

- (d) Keys shall be inventoried with each change of custodian;
- (e) Keys shall not be removed from the premises;
- (f) Keys and spare locks shall be protected in a secure container;
- (g) Locks shall be changed or rotated at least annually, and shall be replaced upon loss or compromise of their keys; and
- (h) Master keying is prohibited.

5-103 Procurement and Phase-In of New Storage Equipment

a. Preliminary Survey. DoD activities shall not procure new storage equipment until:

1. A current survey has been made of on-hand security storage equipment and classified records, and

2. It has been determined, based upon the survey, that it is not feasible to use available equipment or to retire, return, declassify or destroy a sufficient volume of records currently on hand to make the needed security storage space available.

b. Purchase of New Storage Equipment. New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule. Exceptions may be made by heads of Components, with notification to the Deputy Under Secretary of Defense (Policy).

c. Nothing in this chapter shall be construed to modify existing Federal Supply Class Management Assignments made under reference (ai).

5-104 Designations and Combinations

a. Numbering and Designating Storage Facilities. There shall be no external mark as to the level of classified information authorized to be stored therein. For identification purposes each vault or container shall externally bear an assigned number or symbol.

b. Combinations to Containers

1. Changing. Combinations to security containers shall be changed only by individuals having that responsibility and an appropriate security clearance. Combinations shall be changed:

(a) When placed in use;

(b) Whenever an individual knowing the combination no longer requires access;

(c) When the combination has been subject to possible compromise;

(d) At least annually; or

(e) When taken out of service. Built-in combination locks shall be reset to the standard combination 50-25-50: combination padlocks shall be reset to the standard combination 10-20-30.

2. Classifying Combinations. The combination of a vault or container used for the storage of classified information shall be assigned a security classification equal to the highest category of the classified information authorized to be stored therein.

3. Recording Storage Facility Data. A record shall be maintained for each vault, secure room or container used for storing classified information, showing location of the container, the names, home address and home telephone number of the individual having knowledge of the combination.

4. Dissemination. Access to the combination of a vault or container used for the storage of classified information shall be given only to those individuals who are authorized access to the classified information stored therein.

c. Electrically Actuated Locks. Electrically actuated locks (e.g., cypher and magnetic strip card locks) do not afford the required degree of protection of classified information and may not be used as a substitute for the locks prescribed in paragraph 5-102.

5-105 Repair of Damaged Security Containers

Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by authorized persons who are cleared or continuously escorted while so engaged.

a. A GSA-approved security container is considered to have been restored to its original state of security integrity if:

1. All damaged or altered parts (e.g., locking drawer, drawer head, etc.) are replaced; or

2. When a container has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, the replacement lock is equal to the original equipment and the drilled hole is repaired with a tapered case-hardened steel rod (e.g., dowel, drill bit, bearing, etc.) with a diameter slightly larger than the hole and of such length that when driven into the hole there shall remain at each end of the rod a

shallow recess not less than 1/8 inch nor more than 3/16 inch deep to permit the acceptance of substantial welds, and the rod is welded both on the inside and outside surfaces. The outside of the drawer head shall then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts (e.g., new lock).

b. GSA-approved containers which have been drilled in a location or repaired in a manner other than as described in paragraph a., above, will not be considered to have been restored to their original state of security integrity. The "Test Certification Label" on the inside of the locking drawer and the "General Services Administration Approved Security Container" label, if any, on the outside of the top drawer shall be removed from such containers.

c. If damage to a GSA-approved security container is repaired with welds, rivets, or bolts that cannot be removed and replaced without leaving evidence of entry, the cabinet is limited thereafter to the storage of Secret and Confidential material.

d. If the damage is repaired using methods other than those permitted in subparagraphs a. and c. above, use of the container will be limited to unclassified material and a notice to this effect will be permanently marked on the front of the container.

Section 2

CUSTODIAL PRECAUTIONS

5-200 Responsibilities of Custodians

a. Custodians of classified information shall be responsible for providing protection and accountability for such information at all times and for locking classified information in appropriate security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures that ensure that unauthorized persons do not gain access to classified information.

b. Only the head of a activity, or a designee, may authorize removal of classified information from designated working areas in off-duty hours provided that appropriate activity regulations ensure maximum protection possible under the circumstances.

5-201 Care During Working Hours

DoD personnel shall take precaution to prevent unauthorized access to classified information.

a. Classified documents removed from storage shall be kept under constant surveillance and face down or covered when not in use.

b. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, typewriter ribbons, and other items containing classified information shall be either (1) destroyed immediately after they have served their purpose, or (2) shall be given the same classification and secure handling as the classified information they contain.

c. Destruction of typewriter ribbons shall be accomplished in the manner prescribed for classified working papers of the same classification. After the upper and lower sections have been cycled through and overprinted five times in all ribbon or typing positions, fabric ribbons may be treated as unclassified regardless of their classified use thereafter. Carbon and plastic typewriter ribbons and carbon paper that have been used in the production of classified information shall be destroyed in the manner prescribed for working papers of the same classification after initial usage. As an exception to the foregoing, any typewriter ribbon which remains substantially stationary in the typewriter until it has received at least five consecutive impressions may be treated as unclassified.

5-202 End-of-Day Security Checks

Heads of activities shall establish a system of security checks at the close of each working day to ensure that:

- a. All classified material is stored in the manner prescribed;
- b. Burn bags are properly stored or destroyed;
- c. Wastebaskets do not contain classified material; and
- d. Optional Form No. 62 or other designated standard form shall be used by DoD Components for security container check purposes.

5-203 Emergency Planning

a. Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action. Such plans shall establish detailed procedures and responsibilities for the protection of classified material to ensure that it does not come into the possession of unauthorized persons.

b. These emergency planning procedures do not apply to material related to Communications Security (COMSEC). Planning for the emergency protection including emergency destruction under no-notice conditions of classified COMSEC material shall be developed in accordance with the requirements of reference (v).

c. Emergency plans shall provide for the protection of classified material in a manner that will minimize the risk of injury or loss of life to personnel. In the case of fire or natural disaster, the immediate placement of authorized personnel around the affected area, pre-

instructed and trained to prevent the removal of classified material by unauthorized personnel, is an acceptable means of protecting classified material and reducing casualty risk. Such plans shall provide for emergency destruction to preclude capture of classified material when determined to be required. This determination shall be based on an overall commonsense evaluation of the following factors:

1. Level and sensitivity of classified material held by the activity;
 2. Proximity of land-based commands to hostile or potentially hostile forces or to communist-controlled countries;
 3. Flight schedules or ship deployments in the proximity of hostile or potentially hostile forces or near communist-controlled countries;
 4. Size and armament of land-based commands and ships;
 5. Sensitivity of operational assignment. (Contingency planning should also be considered.); and
 6. Potential for aggressive action of hostile forces.
- d. When preparing emergency destruction plans, consideration shall be given to the following:
1. Reduction of the amount of classified material held by a command as the initial step toward planning for emergency destruction;
 2. Storage of less frequently used classified material at more secure commands in the same geographical area (if available);
 3. Transfer of as much as possible of retained classified material to microforms, thereby reducing the bulk that needs to be evacuated or destroyed;
 4. Emphasis on the priorities for destruction, designation of personnel responsible for destruction, and the designation of places and methods of destruction. Additionally, if any destruction site or any particular piece of destruction equipment is to be used by more than one activity or entity, the order or priority for use of the site or equipment must be clearly delineated;
 5. Authorization for the senior individual present in an assigned space containing classified material to deviate from established plans when circumstances warrant; and
 6. Emphasis on the importance of beginning destruction sufficiently early to preclude loss of material. The effect of premature

destruction is considered inconsequential when measured against the possibility of compromise.

e. The emergency plan shall require that classified material holdings be assigned a priority for emergency evacuation or destruction. Priorities should be based upon the potential effect on the national security should such holdings fall into hostile hands, in accordance with the following general guidelines:

1. Priority One. Exceptionally grave damage (Top Secret material);
2. Priority Two. Serious damage (Secret material); and
3. Priority Three. Identifiable damage (Confidential material).

f. If, as determined by appropriate threat analysis, Priority One material cannot otherwise be afforded a reasonable degree of protection from hostile elements in a no-notice emergency situation, then provisions shall be made for installation of Anti-compromise Emergency Destruct (ACED) equipment to ensure timely initiation and positive destruction of such material¹ in accordance with the standard established in subsection III.B., reference (af), i.e., "With due regard for personnel and structural safety, the ACED system shall reach a stage in destruction sequences at which positive destruction is irreversible within 60 minutes at shore installations, 30 minutes in ships, and 3 minutes in aircraft following activation of the ACED system."

g. An ACED requirement is presumed to exist and provision shall be made for an ACED system to protect Priority One material in the following environments:

¹Technological limitations, particularly as to personnel and structural safety, place constraints on the amount of material that can be accommodated in buildings, ships, and aircraft by current ACED systems; therefore, only Priority One material reasonably can be so protected at this time. Nevertheless, after processing Priority One material in an emergency situation involving possible loss to hostile forces, it is imperative that Priority Two material and then Priority Three material be destroyed insofar as is possible by whatever means available.

²The time frames indicated above are those for the initiation of irreversible destruction, not necessarily for the completion of such destruction.

1. Shore-based activities located in or within 50 miles of potentially hostile countries, or located within or adjacent to countries with unstable governments;

2. Reconnaissance aircraft, both manned and unmanned, that operate within JCS-designated reconnaissance reporting areas (see SM 701-76, Volume II, "Peacetime Reconnaissance and Certain Sensitive Operations");

3. Naval surface noncombatant vessels operating in hostile areas when not accompanied by a combatant vessel;

4. Naval subsurface vessels operating in hostile areas; and

5. U.S. Navy "Special Project" ships (Military Sealift Command-operated) operating in hostile areas.

h. Except in the most extraordinary circumstances, ACED is not applicable to commands and activities located within the United States. Should there be reason to believe that an ACED requirement exists in environments other than in those listed in subparagraph g., above, a threat and vulnerability study should be prepared and submitted to the head of the DoD Component concerned or his designee for this purpose, for approval. The threat and vulnerability study should include, as a minimum, the following data, classified if appropriate:

1. Volume and type of Priority One material held by the activity, i.e., paper products, microforms, magnetic tape, circuit boards, etc.;

2. A statement certifying that the amount of Priority One material held by the activity has been reduced to the lowest possible level;

3. An estimate of the time, in excess of the timeframes cited above, required to initiate irreversible destruction of Priority One material held by the activity, and the methods by which destruction of that material would be attempted in the absence of an ACED system;

4. Size and composition of the activity;

5. Location of the activity and the degree of control it, or other United States authority, exercises over security; and

6. Proximity to potentially hostile forces and potential for aggressive action by such forces.

i. When a requirement is believed to exist for ACED equipment not in the General Services Administration or DoD inventories, the potential requirement shall be submitted to the Deputy Under Secretary of Defense

(Policy), for validation in accordance with subsection V. B., reference (af).

j. In determining the method of destruction of other than Priority One material, any method specified for routine destruction or any other means that will ensure positive destruction of the material may be used. Ideally, any destruction method should provide for early attainment of a point at which the destruction process is irreversible. Additionally, classified material may be jettisoned at sea to prevent its easy capture. It should be recognized that such disposal may not prevent recovery of the material. Where none of the methods previously mentioned can be employed, the use of other means, such as dousing the classified material with a flammable liquid and igniting it, or putting to use the facility garbage grinders, sewage treatment plants, boilers, etc., should be considered.

k. Under emergency destruction conditions, destruction equipment would be operated at maximum capacity and without regard to pollution, preventive maintenance, and other restraints that might otherwise be observed.

l. Commands and activities that are required to maintain an ACED system pursuant to subparagraph g., above, shall conduct drills periodically to ensure that responsible personnel are familiar with the emergency plan. Such drills should be used to evaluate the anticipated effectiveness of the plan and the prescribed equipment and should be the basis for improvements in planning and equipment use. Actual destruction should not be initiated during drills.

5-204 Telecommunications Conversations

Classified information shall not be discussed in telephone conversations except as authorized over approved secure communications circuits.

5-205 Security of Meetings and Conferences

Security requirements and procedures governing disclosure of classified information at conferences, symposia, conventions, and similar meetings, as well as requirements governing the sponsorship and attendance at such meetings, is governed by references (x), (aa) and (ab).

³Information on ACED systems may be obtained from the Office of the Chief of Naval Operations, (OP-009D), Navy Department, Washington, D.C. 20350.

COMPROMISE OF CLASSIFIED INFORMATION

6-100 Policy

Compromise of classified information presents a threat to the national security. Once a compromise is known to have occurred the seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise. Where possible, action also should be taken to regain custody of the documents or material which were compromised. In all cases, however, appropriate action must be taken to identify the source and reason for the compromise and remedial action taken to ensure further compromises do not occur. The provisions of reference (f) and (g) apply to compromises covered by this Chapter.

6-101 Cryptographic Information

The procedures for handling compromises of cryptographic information are set forth in reference (v).

6-102 Responsibility of Discoverer

Any person who has knowledge of the actual or possible compromise as defined in paragraph 1-307 of classified information shall immediately report such fact to a responsible official.

6-103 Preliminary Inquiry

A designated responsible official shall initiate a preliminary inquiry to determine the circumstances surrounding an actual or possible compromise. The preliminary inquiry shall establish one of the following:

a. That a compromise of classified information did not occur or that the compromise could not reasonably be expected to cause identifiable damage to the national security. If in such instances, the official finds no indication of significant security weakness, the report of initial inquiry will be sufficient to resolve the incident and, when appropriate, support the administration of disciplinary action;

b. That an actual compromise did occur or that probability of identifiable damage to the national security cannot be discounted. Upon this determination, the responsible official will:

1. Report the circumstances to an appropriate authority as specified in Component instructions;

2. If the responsible official is the originator, he shall take the action prescribed in paragraph 6-106; and

3. If the responsible official is not the originator, notify the originator of the known details of the compromise, including identification of the classified information. If the originator is unknown, notification will be sent to the office specified in Component instructions.

6-104 Investigation

If it is determined that further investigation is warranted, such investigation will include the following:

- a. Complete identification of each item of classified information involved;
- b. A thorough search for the classified information;
- c. Identification of any person or procedure responsible for the compromise. Any person so identified shall be apprised of the nature and circumstances of the compromise and be provided an opportunity to reply to the violation charged. If such person does not choose to make a statement this fact shall be included in the report of investigation;
- d. A statement that compromise occurred or is probable, or a statement that compromise did not occur or that there is minimal risk of damage to the national security; and
- e. Compilation of the data in subparagraphs a. through d. above, in a report to the authority ordering the investigation.

6-105 Responsibility of Authority Ordering Investigation

- a. The report of investigation shall be reviewed to ensure compliance with this Regulation and instructions issued by Components.
- b. The recommendations contained in the report of investigation shall be reviewed to determine sufficiency of remedial, administrative or disciplinary action proposed and, if adequate, the report of investigation forwarded with recommendations through supervisory channels. See paragraphs 14-101 and 14-102.

6-106 Responsibility of Originator

The originator or an official higher in the originator's supervisory chain will, upon receipt of notification of loss or possible compromise of classified information, take action as prescribed in paragraph 2-210 of this Regulation.

6-107 Espionage and Deliberate Compromise

Cases of espionage and deliberate compromise shall be reported in accordance with references (f) and (g) and implementing issuances.

6-108 Unauthorized Absentees

When an individual who has had access to classified information is on unauthorized absence, inquiry, as appropriate under the circumstances, to include consideration of the length of absence and the degree of sensitivity of the classified information involved, shall be conducted to detect if there are any indications of activities, behavior or associations that may be inimical to the interests of national security. Where such indications are detected, a report shall be made to the Component counterintelligence organization.

CHAPTER VII

ACCESS, DISSEMINATION AND ACCOUNTABILITY

Section 1

ACCESS

7-100 Policy

Except as otherwise provided for in paragraph 7-105, no person may have access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties. A personnel security clearance is an indication that the trustworthiness decision has been made. Procedures shall be established by the head of each Component to prevent unnecessary access to classified information. There shall be a demonstrable need for access to classified information before a request for a personnel security clearance can be initiated. The number of people cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs. No one has a right to have access to classified information solely by virtue of rank or position. The final responsibility for determining whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests upon the individual who has authorized possession, knowledge, or control of the information and not upon the prospective recipient. These principles are equally applicable if the prospective recipient is an organizational entity, including commands, other Federal Agencies, Defense contractors, foreign governments, and others.

7-101 Determination of Trustworthiness

a. Except as provided in paragraph 7-106 below, no person shall have access to classified information unless a determination has been made of that person's trustworthiness. This determination, referred to as a security clearance, shall be based on an investigation in accordance with the standards and criteria of reference (h). Interim clearances may be granted in accordance with the provisions of reference (h).

b. United States citizen employees of contractors with classified Government contracts may be granted Confidential clearances by the contractor under the Industrial Security Program, except that such clearances are not valid for Sensitive Compartmented Information, Restricted Data, Cryptographic information, COMSEC information, ACDA, or NATO and CENTO information classified Confidential.

7-102 Continuous Evaluation of Eligibility

a. DoD activities shall report to an appropriate clearing authority information relative to the criteria of reference (h) concerning individuals who are cleared or are in the process of being cleared including contractor personnel cleared under the Defense Industrial Security Program. Reports involving contractor personnel shall be submitted to the Defense Industrial Security Clearance Office, Columbus, Ohio.

b. All DoD activities shall continually evaluate information coming into their possession regarding persons granted security clearances to ensure the criteria cited in DoD Directive 5210.8 continue to be satisfied.

c. Such evaluation is premised upon close coordination with security, personnel, medical, legal and supervisory officials to assure that all information available within a command is evaluated when it pertains to an individual who is cleared or is being considered for clearance.

7-103 Determination of Need-to-Know

In addition to a security clearance, an individual must have a need for access to the classified information or material sought in connection with the performance of official duties or contractual obligations. The determination of that need shall be made as provided in paragraph 7-100 above.

7-104 Revocation of Security Clearance for Cause

A security clearance will be revoked by the appropriate clearing authority when it is determined, in accordance with applicable regulations, that such clearance is no longer clearly consistent with the interests of national security.

7-105 Access by Persons Outside the Executive Branch

Classified information may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Government will derive a benefit or advantage, and that such release is not prohibited by the originating department or agency. Heads of DoD Components shall designate appropriate officials to determine, prior to the release of classified information, the propriety of such action in the interest of national security and assurance of the recipient's trustworthiness and need-to-know.

a. Congress. Access to classified information or material by Congress, its committees, members, and staff representatives shall be in accordance with reference (i). Any DoD employee testifying before a Congressional committee in executive session in relation to a classified matter shall obtain the assurance of the committee that individuals

present have a security clearance commensurate with the highest classification of the information that may be discussed. Members of Congress, by virtue of their elected positions, are not investigated or cleared by the Department of Defense.

b. Government Printing Office (GPO). Documents and material of all classifications may be processed by the GPO, which protects the information in accordance with Department of Defense/Government Printing Office Agreement, dated June 26, 1956.

c. Representatives of the General Accounting Office (GAO). Representatives of the GAO may be granted access to classified information originated by and in possession of the DoD when such information is relevant to the performance of the statutory responsibilities of that office, as set forth in reference (j). Officials of the GAO, as designated in Appendix B, are authorized to certify security clearances, and the basis therefor. Certifications will be made by these officials pursuant to arrangements with the DoD Component concerned. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes.

d. Industrial, Educational and Commercial Entities.

1. Bidders, contractors, grantees, educational, scientific or industrial organizations may have access to classified information only when such access is essential to a function that is necessary in the interest of the national security, and the recipients are cleared in accordance with reference (aa).

2. Contractor employees whose duties do not require access to classified information are not eligible for personnel security clearance and cannot be investigated under the Defense Industrial Security Program. In exceptional situations, where a military command is vulnerable to sabotage and its mission is of critical importance to national security, National Agency Checks may be conducted on such individuals with the approval of the Deputy Under Secretary of Defense (Policy).

e. Historical Researchers. Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that the agency with classification jurisdiction over the information:

1. Makes a written determination that such access is clearly consistent with the interests of national security;

2. Limits such access to specific categories of information over which that agency has classification jurisdiction;

3. Maintains custody of classified information at a DoD installation or activity;

4. Obtains the recipient's agreement to safeguard the information and to authorize a review of any notes and manuscript for determination that no classified information is contained therein by signing a statement entitled "Conditions Governing Access to Official Records for Historical Research Purposes"; and

5. Issues an authorization for access valid for two years from the date of issuance that may be renewed under regulations of the issuing Component.

f. Former Presidential Appointees. Persons who previously occupied policy making positions to which they were appointed by the President, may not remove classified information upon departure from office as all such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information that they originated, received, reviewed, signed, or that was addressed to them while serving as such an appointee, provided that the DoD Component with classification jurisdiction for such information;

1. Makes a written determination that such access is clearly consistent with the interests of national security;

2. Limits such access to specific categories of information over which that agency has classification jurisdiction;

3. Maintains custody of classified information at a DoD installation or activity; and

4. Obtains the recipient's agreement to safeguard the information and to authorize a review of any notes and manuscript for determination that no classified information is contained therein.

g. Judicial Proceedings.

1. An individual or agency receiving an order or subpoena issued by a Federal or State court of record to produce classified information shall immediately refer such order or subpoena to the cognizant Judge Advocate General's or General Counsel's office. Such office shall contact the originator of the information to determine if declassification can be effected.

2. If declassification is not possible, cognizant legal counsel shall take appropriate action to protect such information.

3. If no alternative exists to release of such information for use in a judicial proceeding, cognizant legal counsel shall take all proper steps to ensure the cooperation of the court and opposing counsel in safeguarding and retrieving the information. It shall be recommended to the court that the following minimum security safeguards be included in a court order:

(a) Every effort shall be made to limit dissemination to in camera review by the Judge of the court of record to determine the relevancy of the information in question.

(b) Classified material will not be authorized for introduction into evidence at a civil trial before a jury. Attendance at any proceeding where classified information is to be introduced shall be limited to the presiding judge of a court and those attorneys and other persons whose duties require knowledge or possession of the information and who have been cleared by DoD.

(c) All proceedings shall be held in a secured court or hearing room pursuant to DoD security procedures and regulations.

(d) Dissemination and accountability controls must be established for all classified information marked for identification or offered or introduced into evidence.

(e) The transcript of the proceeding shall be appropriately marked to show the classified portions.

(f) All classified information shall be handled and stored in a manner consistent with DoD security procedures.

(g) Any notes, drafts, or other documents produced by non-DoD individuals, no longer required by any party to the proceeding shall be transferred to the DoD for destruction.

(h) All recipients of classified information disclosed under the provisions of this section shall be advised of the classification level, safeguarding and storage requirements, and their liability in the event of unauthorized disclosure.

(i) At the conclusion of the proceeding, all classified information must be returned to the DoD or placed under seal of the Court of Record.

4. This subparagraph shall not apply to litigation arising under the Freedom of Information Act, 5 U.S.C. Par 552, as amended.

7-106 Access by Foreign Nationals, Foreign Governments, International Organizations, and Immigrant Aliens

a. Classified information may be released to foreign nationals, foreign governments and international organizations, only when authorized under the provisions of the National Disclosure Policy and reference (1); and

b. Secret and Confidential information may be released to immigrant aliens who reside and intend to reside permanently in the United States, in the performance of official duties, provided they have been granted a security clearance based upon a favorable Background Investigation.

c. Immigrant aliens may be granted a Limited Access Authorization to Top Secret information for a specific contract or program provided that the head of the Component concerned makes a personal written determination that such access is essential to meet Government requirements and that the individual is reliable and trustworthy in accordance with reference (h). A report of each such determination shall be furnished to the Deputy Under Secretary of Defense (Policy).

c. Access to COMSEC information by persons and activities subject to this paragraph shall be in accordance with policy issuances of the National Communications Security Committee (NCSC).

7-107 Other Situations

When necessary in the interests of national security heads of DoD Components, or their single designee, may authorize access by persons outside the Federal Government, other than those enumerated in paragraphs 7-105 and 7-106, to classified information upon determining that (a) the recipient is trustworthy for the purpose of accomplishing a national security objective and (b) that the recipient can and will safeguard the information from unauthorized disclosure.

7-108 Access Required by Other Executive Branch Investigative and Law Enforcement Agents

a. Normally, investigative agents of other departments or agencies may obtain access to DoD information through established liaison or investigative channels.

b. When the urgency or delicacy of a Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), or Secret Service investigation precludes use of established liaison or investigative channels, FBI, DEA or Secret Service agents may obtain access to DoD information as required. However, this information shall be protected as required by its classification. Prior to any public release of the information so obtained the approval of the head of the activity or higher authority shall be obtained.

Section 2

DISSEMINATION

7-200 Policy

Components shall establish procedures consistent with this Regulation for the dissemination of classified material. The originating official or activity may prescribe specific restrictions on dissemination of classified information when necessary.

7-201 Restraints on Special Access Requirements

Special requirements with respect to access, distribution and protection of classified information shall require prior approval in accordance with Chapter XII.

7-202 Information Originating in a Non-DoD Department or Agency

Except under rules established by the Secretary of Defense, or as provided by Section 102 of the National Security Act, 50 U.S.C. Section 403, classified information originating in a department or agency other than DoD shall not be disseminated outside the DoD without the consent of the originating department or agency.

7-203 Foreign Intelligence Information

Dissemination of foreign intelligence information shall be in accordance with the provisions of reference (m).

7-204 Restricted Data and Formerly Restricted Data

Information bearing the warning notices prescribed in paragraphs 4-501 and 4-502 shall not be disseminated outside authorized channels without the consent of the originator. Access to and dissemination of Restricted Data by DoD personnel shall be subject to reference (n).

7-205 NATO and CENTO Information

Classified information originated by NATO or CENTO shall be safeguarded in accordance with references (o) and (p).

7-206 COMSEC Information

COMSEC information shall be disseminated in accordance with reference (v).

7-207 Dissemination of Top Secret Information

a. Top Secret information, originated within the DoD, may not be disseminated outside the DoD without the consent of the originating DoD Component, or higher authority.

b. Top Secret information, whenever segregable from classified portions bearing lower designations, shall be distributed separately.

7-208 Dissemination of Secret and Confidential Information

Classified information other than Top Secret, originated within DoD, may be disseminated within the Executive Branch, unless prohibited by the originator. (See paragraph 4-505.)

7-209 Restraint on Reproduction

Portions of documents and materials that contain Top Secret information shall not be reproduced without the consent of the originator or higher authority. Any stated prohibition against reproduction shall be strictly observed. (See paragraph 4-505.) The following measures apply to reproduction equipment and to the reproduction of classified information:

- a. Copying of documents containing classified information shall be minimized;
- b. Officials authorized to approve the reproduction of Top Secret and Secret information shall be designated by position title and shall review the need for reproduction of classified documents with a view toward minimizing reproduction;
- c. Specific reproduction equipment shall be designated for the reproduction of classified information. Rules for reproduction of classified information shall be posted on or near the designated equipment;
- d. Notices prohibiting reproduction of classified information shall be posted on equipment used only for the reproduction of unclassified information;
- e. Components shall ensure that equipment used for reproduction of classified material does not leave latent images in the equipment or on other material;
- f. All copies of classified documents reproduced for any purpose including those incorporated in a working paper are subject to the same controls prescribed for the document from which the reproduction is made; and
- g. Records shall be maintained to show the number and distribution of reproduced copies of all Top Secret documents, of all classified documents covered by special access programs distributed outside the originating agency, and of all Secret and Confidential documents which are marked with special dissemination and reproduction limitations. (See paragraph 4-505.)

7-210 Code Words, Nicknames and Exercise Terms

The use of code words, nicknames and exercise terms are subject to Appendix C.

7-211 Scientific and Technical Meetings

Use of classified information in scientific and technical meetings is subject to reference (x).

ACCOUNTABILITY AND CONTROL

7-300 Top Secret Information

DoD activities shall establish the following procedures:

a. Control Officers. Top Secret Control Officers, and alternates, shall be designated within offices to be responsible for receiving, dispatching, and maintaining accountability registers of Top Secret documents. Such individuals shall be selected on the basis of experience and reliability, and shall have appropriate security clearances.

b. Accountability. Top Secret accountability registers shall be maintained by each originating and recipient office for all Top Secret documents and material in its custody. The name and title of all individuals, including stenographic and clerical personnel to whom information in such documents and materials has been disclosed, and the date of such disclosure, shall be recorded therein. Disclosures to individuals who may have had access to containers in which Top Secret information is stored, or who regularly handled a large volume of such information, need not be so recorded. Such individuals, when identified on a roster, are deemed to have had access to such information on the listed date. Disclosure records shall be retained for 2 years after the documents or materials are transferred, downgraded, or destroyed.

c. Inventories. Top Secret documents and material shall be inventoried at least once annually. At such time, each document or material shall be examined for completeness and accuracy. Repositories, libraries, or activities which store large volumes of classified information, however, may limit their annual inventory to documents and material which have been disclosed within the past year, and 10 percent of the remaining inventory. If a storage system contains large volumes of information and security measures are adequate to prevent access by unauthorized persons, a request for waiver of the annual inventory requirement accompanied by full justification may be submitted to the Deputy Under Secretary of Defense (Policy).

d. Retention. Top Secret documents shall be reproduced and retained only to the extent necessary to satisfy current requirements. Custodians shall destroy non-record copies of Top Secret documents when no longer needed. Record copies of documents that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to designated records centers.

e. Receipts. Top Secret documents and material will be accounted for by a continuous chain of receipts.

f. Serialization. Copies of Top Secret documents and material shall be numbered serially.

7-301 Secret Information

Administrative procedures shall be established controlling Secret material (a) originated or received by an activity; (b) distributed or routed to a subelement of such activity; and (c) disposed of by the activity by transfer of custody or destruction. The control system for Secret must be determined by the practical balance of security and operating efficiency.

7-302 Confidential Information

Administrative controls shall be established to protect Confidential information received, originated, transmitted or stored by an activity.

7-303 Receipt of Classified Material

Procedures shall be developed within DoD activities to protect incoming mail, bulk shipments, and items delivered by messenger until a determination is made whether classified information is contained therein. Screening points shall be established to limit access to classified information to cleared personnel.

7-304 Working Papers

a. General Requirements. Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be:

1. Dated when created;
2. Marked with the highest classification of any information contained therein;
3. Protected in accordance with the assigned classification;
4. Destroyed when no longer needed;
5. Marked with a declassification or review date when placed in permanent files; and
6. Accounted for and controlled in the manner prescribed for a finished document of comparable classification when:

(a) Released by the originator outside a headquarters or transmitted through message center channels within a headquarters;

(b) Filed permanently; or

(c) Retained more than 180 days from date of origin.

b. Special Requirements for Top Secret. Top Secret working papers shall be stored as prescribed in subparagraph 5-102a. At the end of each duty day they shall be returned to the custody of the Top Secret control officer.

CHAPTER VIII

TRANSMISSION

Section 1

METHODS OF TRANSMISSION OR TRANSPORTATION

8-100 Policy

Classified information may be transmitted or transported only as specified in this chapter.

8-101 Top Secret Information

Transmission of Top Secret information shall be effected only by:

- a. The Armed Forces Courier Service (ARFCS),
- b. Authorized Component Courier Services,
- c. If appropriate, the Department of State Courier System,
- d. Cleared and designated personnel traveling on a conveyance owned, controlled or chartered by the Government or DoD contractors,
- e. Cleared and designated U.S. Military personnel and Government civilian employees by surface transportation,
- f. Cleared and designated U.S. Military personnel and Government civilian employees on scheduled commercial passenger aircraft within and between the United States, its Territories and Canada,
- g. Cleared and designated DoD contractor employees within and between the United States and its Territories provided that: the transmission has been authorized in writing by the appropriate contracting officer or his designated representative and, the designated employees have been briefed in their responsibilities as couriers or escorts for the protection of Top Secret material. Complete guidance for Top Secret transmission is specified in references (aa) and (ab).
- h. A cryptographic system authorized by the Director, NSA, or via a protected distribution system designed and installed to meet the standards included in the National COMSEC and Emanations Security (EMSEC) Issuance System.

Transmission of Secret information may be effected by:

a. Any of the means approved for the transmission of Top Secret information except that Secret information may be introduced into the Armed Forces Courier Service (ARFCOS) only when the control of such information cannot be otherwise maintained in U.S. custody. This restriction does not apply to Sensitive Compartmented Information and COMSEC information.

b. Appropriately cleared contractor employees within and between the United States and its Territories provided that: (1) the designated employees have been briefed in their responsibilities as couriers or escorts for protecting Secret information; (2) the classified information remains under the constant custody and protection of the contractor personnel at all times; and (3) the transmission otherwise meets the requirements specified in references (aa) and (ab). In other areas, appropriately cleared DoD contractor employees may transmit Secret information only when: (1) the information is not transported across international borders; (2) time limitations do not permit the use of U.S. Government channels; (3) the transmission is begun and completed during normal duty hours of the same day and by surface means only; and (4) the transmission otherwise meets the requirements specified in references (aa) and (ab);

c. United States Postal Service registered mail within and between the United States and its Territories;

d. United States Postal Service registered mail through Army, Navy, or Air Force Postal Service facilities, outside the United States and its Territories provided that the information does not at any time pass out of United States citizen control and does not pass through a foreign postal system or any foreign inspection;

e. United States Postal Service and Canadian registered mail with registered mail receipt between United States Government and Canadian government installations in the United States and Canada;

f. Carriers authorized to transport Secret information via a Protective Security Service (PSS) under the Department of Defense Industrial Security Program. This method is authorized only within the United States boundaries and only when the size, bulk, weight, nature of the shipment, or escort considerations make the use of other methods impractical. Routings for these shipments will be obtained from the Military Traffic Management Command;

g. The following carriers under appropriate escort: Government and Government contract vehicles including aircraft, ships of the United States Navy, civil service operated United States Naval ships, and ships of U.S. registry. Appropriately cleared operators of vehicles, officers

of ships or pilots of aircraft who are United States citizens may be designated as escorts provided the control of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access. However, observation of the shipment is not required during the period it is stored in an aircraft or ship in connection with flight or sea transit, provided the shipment is loaded into a compartment that is not accessible to any unauthorized persons or in a specialized secure, safe-like container that is:

1. Constructed of solid building material that provides a substantial resistance to forced entry;
2. Constructed in a manner that precludes surreptitious entry through disassembly or other means, and that attempts at surreptitious entry would be readily discernible through physical evidence of tampering; and
3. Secured by a numbered cable seal lock affixed to a high security hasp. The hasp must be installed in a manner that precludes surreptitious removal.

h. Use of specialized containers aboard aircraft requires that:

1. Appropriately cleared personnel maintain observation of the material as it is being loaded aboard the aircraft and that observation of the aircraft continues until it is airborne;
2. Observation by appropriately cleared personnel is maintained at the destination as the material is being off-loaded and at any intermediate stops. Observation will be continuous until custody of the material is assumed by appropriately cleared personnel.

8-103 Confidential Information

Transmission of Confidential information may be effected by:

a. Means approved for the transmission of Secret information. However, United States Postal Service registered mail shall be used for Confidential only as indicated in subparagraph b below;

b. United States Postal Service registered mail for:

1. Confidential information of NATO and CENTO;
2. Other Confidential material to and from FPO or APO addressees located outside the United States and its Territories;
3. Other addressees when the originator is uncertain that their location is within the United States boundaries. Use of return postal receipts on a case by case basis is authorized.

c. United States Postal Service First Class Mail between Department of Defense Component locations anywhere in the United States and its Territories. However, the outer envelope/wrappers of such Confidential material shall be endorsed "Postmaster: Do Not Forward, Return to Sender." Certified or, if appropriate, registered mail shall be used for material directed to DoD contractors and to non-DoD agencies of the Executive Branch. United States Postal Service Express Mail Service may be used between DoD Component locations, between DoD contractors, and between DoD Components and DoD contractors.

d. Within United States boundaries, commercial carriers that provide a Signature Security Service (SSS). Information concerning commercial carriers that provide SSS may be obtained from the Military Traffic Management Command (MTMC).

e. In the custody of commanders or masters of ships of United States registry who are United States citizens. Confidential information shipped on ships of United States registry may not pass out of United States Government control. The commanders or masters must give and receive classified information receipts and agree to:

1. Deny access to the Confidential material by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspection will not be unloaded; and

2. Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

f. Such alternative or additional methods of transmission as the head of any Component may establish by rule or regulation, provided those methods afford at least an equal degree of security.

8-104 Transmission of Classified Information to Foreign Governments

a. Subsequent to a determination by competent authority that classified information may be released to a foreign government, it shall be transmitted only:

1. To an embassy or official agency or representative of the recipient government, or

2. For on-loading aboard a ship, aircraft or other carrier designated by the recipient government at the point of departure from the United States, or its territories, provided that at the time of delivery a duly authorized representative of the recipient government is present at the point of departure to accept delivery, to ensure immediate loading, and to assume security responsibility for the classified materia

b. Classified material shall be transferred on a government-to-government basis by duly authorized representatives of each government, and shall not pass to a foreign government until a delivery receipt, to include a United States postal receipt where applicable, has been executed by a duly authorized representative of the recipient foreign government.

c. Each contract, agreement or arrangement that contemplates transfer of classified material to a foreign government at a point within the United States, its Territories or possessions, shall designate a point of delivery in accordance with subparagraphs a.1. or a.2. above. If delivery is to be at a point as described in subparagraph a.2. above, the contract, agreement or arrangement shall provide for:

1. United States Government storage, or

2. Storage by a cleared commercial carrier or other U.S. cleared storage point, or

3. Storage at a storage point owned or controlled by the recipient foreign government, at or near the delivery point so that the classified material may be temporarily stored in the event the carrier designated by the recipient foreign government is not available for loading.

4. Storage facilities used or designated must afford the classified material the protection required by this Regulation. Any storage facility referred to in subparagraph 3 above shall be protected by a trained guard force consisting of nationals of the recipient government, or U.S. citizens for whom security assurances have been provided by the Department of Defense to the recipient foreign government. In addition, an industrial security representative of the Defense Contract Administration Services Region (DCASR) located in the geographical area will, upon request, visit the storage facility and furnish guidance with regard to the physical safeguards required. Continued inspection to ensure the facility is continuing to provide protection required by this Regulation will be made by a DCASR with the cooperation of the foreign government concerned.

d. Classified material to be delivered to a foreign government within the recipient country shall be transmitted in accordance with the provisions of this Chapter. Unless the material is accompanied by a designated or approved courier or escort, it shall, on arrival in the recipient country, be delivered to a United States Government representative who shall arrange for transfer to a duly authorized representative of the recipient foreign government.

e. Classified material to be delivered to the representative of a foreign government within a third country shall be delivered by a U.S. courier or escort to such representative at an agency or installation of the United States or of the recipient country that has extraterritorial status or is otherwise exempt from the jurisdiction of the third country.

8-105 Consignor-Consignee Responsibility for Shipment of Bulky Material

The consignor of a bulk shipment shall:

a. Normally, select a carrier that will provide a single line service from the point of origin to destination, when such a service is available;

b. Ship packages weighing less than 200 pounds in closed vehicles only;

c. Notify the consignee, and military transshipping activities, of the nature of the shipment (including level of classification), the means of shipment, the number of seals, if used, and the anticipated time and date of arrival by separate communication at least 24 hours in advance of arrival of the shipment. Advise the first military transshipping activity that, in the event the material does not move on the conveyance originally anticipated, the transshipping activity should so advise the consignee with information of firm transshipping date and estimated time of arrival. Upon receipt of the advance notice of a shipment of classified material, consignees and transshipping activities shall take appropriate steps to receive the classified shipment and to protect it upon arrival.

d. Annotate the bills of lading to require the carrier to notify the consignor immediately, by the fastest means, if the shipment is unduly delayed enroute. Such annotations shall not, under any circumstances, disclose the classified nature of the commodity. When seals are used annotate substantially as follows:

DO NOT BREAK SEALS EXCEPT IN EMERGENCY OR UPON
AUTHORITY OF CONSIGNOR OR CONSIGNEE. IF BROKEN
APPLY CARRIER'S SEALS AS SOON AS POSSIBLE AND
IMMEDIATELY NOTIFY CONSIGNOR AND CONSIGNEE.

e. Require the consignee to advise the consignor of any shipment not received more than 48 hours after the estimated time of arrival furnished by the consignor or transshipping activity. Upon receipt of such notice, the consignor shall immediately trace the shipment. If there is evidence that the classified material was subjected to compromise, the procedures set forth in Chapter VI of this Regulation for reporting compromises shall apply.

8-106 Transmission of Communications Security (COMSEC) Information

Communications Security (COMSEC) information shall be transmitted in accordance with reference (v).

Restricted Data shall be transmitted in the same manner as other information of the same security classification. The transporting and handling of nuclear weapons or nuclear components shall be in accordance with references (aj) and (ak) and applicable Component directives.

Section 2

PREPARATION OF MATERIAL FOR TRANSMISSION OR SHIPMENT

8-200 Envelopes or Containers

a. Whenever classified information is transmitted, it shall be enclosed in two opaque sealed envelopes or similar wrappings where size permits, except as provided below.

b. Whenever classified material is transmitted of a size not suitable for transmission in accordance with subparagraph a. above, it shall be enclosed in two opaque sealed containers, such as boxes or heavy wrappings.

1. If the classified information is an internal component of a packageable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information.

2. If the classified material is an inaccessible internal component of a bulky item of equipment that is not reasonably packageable the outside or body of the item may be considered to be a sufficient enclosure provided the shell or body does not reveal classified information.

3. If the classified material is an item or equipment that is not reasonably packageable and the shell or body is classified it shall be concealed with an opaque covering that will hide all classified features.

4. Specialized shipping containers, including closed cargo transporters, may be used in lieu of the above packaging requirements. In such cases, the container may be considered the outer wrapping or cover.

c. Material used for packaging shall be of such strength and durability as to provide security protection while in transit, to prevent items from breaking out of the container, and to facilitate the detection of any tampering with the container. The wrappings shall conceal all classified characteristics.

d. Closed and locked vehicles or compartments, or cars shall be used for shipments of classified information except when another method is authorized by the consignor. In any event, individual packages weighing less than 200 pounds gross shall be shipped only in a closed vehicle.

e. To minimize the possibility of compromise of classified material caused by improper or inadequate packaging thereof, responsible officials shall ensure that proper wrappings are used for mailable bulky packages. Responsible officials shall require the inspection of bulky packages to determine whether the material is suitable for mailing or whether it should be transmitted by other approved means.

8-201 Addressing

a. Classified information shall be addressed to an official Government activity or DoD contractor with a facility clearance and not to an individual. This is not intended, however, to prevent use of office code numbers or such phrases in the address as "Attention: Research Department," or similar aids in expediting internal routing, in addition to the organization address.

b. Classified written information shall be folded or packed in such a manner that the text will not be in direct contact with the inner envelope or container. A receipt form shall be attached to or enclosed in the inner envelope or container for all 'Secret and Top Secret information; Confidential information will require a receipt only if the originator deems it necessary. The mailing of written materials of different classifications in a single package should be avoided. However, when written materials of different classifications are transmitted in one package, they shall be wrapped in a single inner envelope or container. A receipt listing all classified information for which a receipt is requested shall be attached or enclosed. The inner envelope or container shall be marked with the highest classification of the contents.

c. The inner envelope or container shall show the address of the receiving activity, classification, including, where appropriate, the "Restricted Data" marking, and any applicable special instructions. It shall be carefully sealed to minimize the possibility of access without leaving evidence of tampering.

d. An outer or single envelope or container shall show the complete and correct address and the return address of the sender.

e. An outer cover or single envelope or container shall not bear a classification marking, a listing of the contents divulging classified information, or any other unusual data or marks that might invite special attention to the fact that the contents are classified.

f. Care must be taken to ensure that classified information intended only for the United States elements of international staffs or other organizations is addressed specifically to those elements.

8-202 Receipt Systems

a. Top Secret information shall be transmitted under a chain of receipts covering each individual who gets custody.

b. Secret information shall be covered by a receipt between activities and other authorized addressees.

c. Receipts for Confidential information are optional.

d. Receipts shall be provided by the transmitter of the material and the forms shall be attached to the inner cover.

1. Postcard receipt forms may be used.

2. Receipt forms shall be unclassified and contain only such information as is necessary to identify the material being transmitted.

3. Receipts shall be retained for at least two years.

e. In those instances where a fly-leaf (page check) form is used with classified publications the postcard receipt will not be required.

8-203 Exceptions

Exceptions may be authorized to the requirements contained in this Chapter by the head of the component concerned or his designee, provided the exception affords equal protection and accountability to that provided above. Proposed exceptions that do not meet these minimum standards shall be submitted to the Deputy Under Secretary of Defense (Policy) for approval.

Section 3

RESTRICTIONS, PROCEDURES AND AUTHORIZATION CONCERNING ESCORT/ HAND-CARRYING OF CLASSIFIED INFORMATION

8-300 General Restrictions

Appropriately cleared personnel may be authorized to escort/hand-carry classified material between their duty station and an activity to be visited subject to the following conditions:

a. The storage provisions of Section I, Chapter V of this Regulation shall apply at all stops enroute to the destination, unless the information is retained in the personal possession and constant surveillance of the individual at all times. The hand carrying of classified information on trips that involve an overnight stopover is not permissible without advance arrangements for proper overnight storage in a Government installation or a cleared contractor's facility.

b. Classified material shall not be read, studied, displayed, or used in any manner in public conveyances or places.

c. When classified material is carried in a private, public, or Government conveyance, it shall not be stored in any detachable storage compartment such as automobile trailers, luggage racks, aircraft travel pods or drop tanks.

d. Responsible officials shall provide a written statement to all individuals escorting or carrying classified material aboard commercial passenger aircraft authorizing such transmission. This authorization statement may be included in official travel orders and should ordinarily permit the individual to pass through passenger control points without the need for subjecting the classified material to inspection. Specific procedures for carrying classified documents aboard commercial aircraft are contained in Section 4, below.

e. Each activity shall list all classified information carried or escorted by travelling personnel. All classified information shall be accounted for.

f. Individuals authorized to carry or escort classified material shall be fully informed of the provisions of this Chapter prior to departure from their duty station.

8-301 Restrictions on Hand-carrying Classified Information Aboard Commercial Passenger Aircraft

Classified information shall not be hand-carried aboard commercial passenger aircraft unless:

1. There is neither time nor means available to move the information in the time required to accomplish operational objectives or contract requirements, including request-for-quotation (RFQ) and request-for-bid (RFB).

2. The hand-carry has been authorized by an appropriate official in accordance with paragraph 8-303, below.

3. In the case of the hand-carry of classified information across international borders, arrangements have been made to ensure that such information will not be opened by customs, border, postal, or other inspectors, either U.S. or foreign.

4. The hand-carry is accomplished aboard a U.S. carrier. Foreign carriers will be utilized only when no U.S. carrier is available and then the approving official must ensure that the information will remain in the custody and physical control of the U.S. escort at all times.

8-302 Procedures for Hand-carrying Classified Information on Commercial Passenger Aircraft

a. Basic Requirements

1. Advance and continued coordination by the DoD activity and contractor officials shall be made with departure airline and terminal officials and, where possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of this issuance and FAA guidance. Specifically, a determination should be made beforehand as to whether documentation described in subparagraph d., below will be required. Local Federal Aviation Administration Security Officers can be of assistance in making this determination. As an aid in coordination and planning, a listing of FAA field offices is at Appendix D.

2. The individual designated as courier shall be in possession of either DD Form 2 (any color) or other DoD or contractor picture identification card and written authorization to carry classified information.

3. The courier shall be briefed as to the provisions of this Chapter.

b. Procedures for Carrying Classified Information in Envelopes

Persons carrying classified information should process through the airline ticketing and boarding procedure in the same manner as all other passengers except for the following:

1. The classified information being carried shall contain no metal bindings and shall be contained in sealed envelopes. Should such envelopes be contained in a briefcase or other carry-on luggage, the briefcase or luggage shall be routinely offered for opening for inspection for weapons. The screening officials may check envelope by X-ray machine, flexing, feel, weight, etc., without opening the envelopes themselves.

2. Opening or reading of the classified document by the screening official is not permitted.

c. Procedures for Transporting Classified Information in Packages

Classified information in sealed or packaged containers shall be processed as follows:

1. The Government or contractor official who has authorized the transport of the classified information shall notify the appropriate air carrier in advance.

2. The passenger carrying the information shall report to the affected airline ticket counter prior to boarding, present his documentation, and the package or cartons to be exempt from screening. The airline representative will review the documentation and description of the containers to be exempt.

3. If satisfied with the identification of the passenger and his documentation, the official will provide the passenger with an escort to the screening station and authorize the screening personnel to exempt the container from physical or other type inspection.

4. If the airline official is not satisfied with the identification of the passenger and/or the authenticity of his documentation, the passenger will not be permitted to board, and not be subject to further screening for boarding purposes.

5. The actual loading and unloading of the information will be under the supervision of a representative of the air carrier; however, appropriately cleared personnel shall accompany the material and keep it under surveillance during loading and unloading operations. In addition, appropriately cleared personnel must be available to conduct surveillance at any intermediate stops where the cargo compartment is to be opened.

6. DoD Components and contractor officials shall establish and maintain appropriate liaison with local FAA officials, airline representative and airport terminal administrative and security officials. Prior notification is emphasized to ensure that the airline representative can make timely arrangements for courier screening.

d. Documentation

1. When authorized to carry sealed envelopes or containers containing classified information both Government and contractor personnel shall present an identification card carrying a photograph, descriptive data, and signature of the individual. (If the identification card does not contain date of birth, height, weight, and signature, these items must be included in the written authorization.)

a. DoD personnel shall present an official identification issued by an agency of the U.S. Government.

b. Contractor personnel shall present identification issued by the contractor or the U.S. Government. Contractors' identification cards shall carry the name of the employing contractor, or otherwise be marked to denote "contractor."

c. The courier shall have the original of a letter authorizing the individual to carry classified information. A reproduced copy is not acceptable; however, the traveler shall have sufficient authenticated copies to provide a copy to each airline involved. The letter shall be prepared on letterhead stationary of the agency or contractor authorizing the carrying of classified material. In addition, the letter shall:

(1) Give the full name of the individual and his employing agency or company;

(2) Describe the type of identification the individual will present (e.g., Naval Research Laboratory Identification Card, No. 1234; ABC Corporation Identification Card No. 1234);

(3) Describe the material being carried (e.g., three sealed packages, 9" x 8" x 24", addressee and addressor);

(4) Identify the point of departure, destination and known transfer points;

(5) Carry a date of issue and an expiration date;

(6) Carry the name, title, and signature of the official issuing the letter. Each package or carton to be exempt shall be signed on its face by the official who signed the letter; and

(7) Carry the name of the Government agency designated to confirm the letter of authorization, and its telephone number. The telephone number of the agency designated shall be an official U.S. Government number

2. Information relating to the issuance of DoD identification cards is contained in reference (a). The Green, Gray, and Red forms of DD Form 2 and other DoD and contractor picture-ID card are acceptable to FAA. Components shall provide for the issuance of DD Form 1173 to civilian employees selected for courier duties, if individuals have not been issued other acceptable ID cards.

(3) The Director, DLA, shall provide for the issuance of DLA/ID card or DD Form 1173 when required by contractor employees selected for courier or hand-carrying duties, when the employer involved does not have an appropriate identification medium.

a. Within the United States, its Territories and Canada

1. Officials within DoD Components who have been authorized to approve travel orders and designate couriers may approve the escort/hand-carry of classified information within the United States, its Territories and Canada.

2. The Director, DLA, shall provide through the DCASR for authorization for contractor personnel to hand-carry classified material.

b. Outside the United States, its Territories and Canada

The head of a DoD Component, or his single designee, may authorize the escort/hand-carry of classified information outside the area encompassed by the United States, its Territories and Canada.

CHAPTER IX

DISPOSAL AND DESTRUCTION

9-100 Policy

Documentary record information originated or received by a Component in connection with the transaction of public business, and preserved as evidence of the organization, functions, policies, operations, decisions, procedures, or other activities of any department or agency of the Government, or because of the informational value of the data contained therein, may be disposed of or destroyed only in accordance with DoD Component record management regulations. Nonrecord classified information and other material of similar temporary nature, shall be destroyed when no longer needed under procedures established by the head of the cognizant Component consistent with the following requirements.

9-101 Methods of Destruction

Classified documents and material shall be destroyed by burning or, with the approval of the cognizant Component head or designee, by melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation sufficient to preclude recognition or reconstruction of the classified information.

9-102 Records of Destruction

a. Records of destruction are required for Top Secret and Secret information. The record shall be dated and signed at the time of destruction by two witnesses for Top Secret information and one witness for Secret. In the case of information placed in burn bags for central disposal, the destruction record need only be signed by the witnessing official or officials when the information is so placed.

b. Records of destruction shall be maintained for a minimum of two years. In individual cases involving Secret information, a cognizant Component head or designees may waive the requirement for destruction records if compliance would create an unacceptable degree of operating inefficiency.

9-103 Classified Waste

Waste material, such as handwritten notes, carbon paper, typewriter ribbons, working papers, etcetera, which contains classified information must be protected in a manner to prevent unauthorized disclosure of the information. Classified waste shall be destroyed, when no longer needed, by a method described in paragraph 9-101. Destruction records are not required.

CHAPTER X

SECURITY EDUCATION

10-100 Responsibility and Objectives

Heads of DoD Components shall establish security education programs for their personnel. Such programs shall stress the objectives of classifying less information, declassifying more, and improving protection of information that requires it. They shall also place emphasis on the balance between the need to release the maximum information appropriate under the Freedom of Information Act and the interest of the Government in protecting the national security.

10-101 Scope and Principles

The security education program shall include all personnel authorized or expected to be authorized access to classified information. Each Component shall design its program to fit the requirements of different groups of personnel. Care must be exercised to assure that the program does not evolve into a perfunctory compliance with formal requirements without achieving the real goals of the program. The program shall, as a minimum, be designed to:

- a. Advise personnel of the adverse effects to the national security that could result from unauthorized disclosure and of their personal, moral, and legal responsibility to protect classified information within their knowledge, possession, or control;
- b. Indoctrinate personnel in the principles, criteria, and procedures for the classification, downgrading, declassification, marking, and dissemination of information, as prescribed in this Regulation, and alert them to the strict prohibitions on improper use and abuse of the classification system;
- c. Familiarize personnel with procedures for challenging classification decisions believed to be improper or to prolong classification unnecessarily;
- d. Familiarize personnel with the security requirements of their particular assignment;
- e. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility to report such attempts;
- f. Advise personnel of the penalties for engaging in espionage activities;

g. Advise personnel of the strict prohibition against discussing classified information over an unsecure telephone or in any other manner that permits interception by unauthorized persons;

h. Inform personnel of the penalties for willful violation or disregard of the provisions of this Regulation;

i. Instruct personnel that individuals having knowledge, possession, or control of classified information must determine, prior to disseminating such information, that the prospective recipient (i) has been cleared for access by competent authority, (ii) needs the information in order to perform his official duties and (iii) can properly protect (or store) the information.

10-102 Refresher Briefings

Programs shall be established to provide periodic security training for personnel having continued access to classified information. The elements outlined in paragraph 10-101, above, shall be tailored to fit the needs of experienced personnel.

10-103 Foreign Travel Briefing

Personnel who have had access to classified information shall be given a Foreign Travel Briefing, prior to travel, to alert them of their possible exploitation under the following conditions:

a. Travel to or through Communist-controlled countries.

b. Attendance at international scientific, technical, engineering or other professional meetings in the United States or in any country outside the United States where it can be anticipated that representatives of Communist-controlled countries will participate or be in attendance. (See also reference (aa)).

c. Individuals who frequently travel, or attend or host meetings of foreign visitors of the types described in subparagraph b. need not be briefed for each such occasion, but shall be provided a thorough briefing at least once each six-month period and a general reminder of security responsibilities prior to each such activity.

10-104 Debriefings

a. Upon termination of employment or contemplated absence from duty or employment for sixty days or more, military members and employees shall be debriefed, return all classified material, and execute a Security Termination Statement. This statement shall include:

1. An acknowledgment that the individual has read the appropriate provisions of the Espionage Act, other criminal statutes, DoD regulations

applicable to the level of classified information to which the individual has had access, and understands the implications thereof;

2. A declaration that the individual no longer has any documents or material containing classified information in his possession;

3. An acknowledgement that the individual will not communicate or transmit classified information to any unauthorized person or agency; and

4. An acknowledgement that the individual will report without delay to the Federal Bureau of Investigation or the DoD Component concerned any attempt by any unauthorized person to solicit classified information.

b. When an individual refuses to execute a debriefing statement, that fact shall be reported immediately to the security office of the cognizant organization concerned.

c. The Security Termination Statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's records retention schedules, but for a minimum of two years after the individual is debriefed.



CHAPTER XI

FOREIGN GOVERNMENT INFORMATION

Section 1 CLASSIFICATION

11-100 Classification

a. Foreign government information classified by a foreign government or international organization of governments shall retain its original classification designation or be assigned a United States classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.

b. Foreign government information that was not classified by a foreign entity but was provided with the expectation, expressed or implied, that it be held in confidence must be classified. The two-step procedure for classification prescribed in paragraph 2-202 does not apply to the classification of such foreign government information because Executive Order 12065 (reference (b)) states a presumption of at least identifiable damage to the national security in the event of unauthorized disclosure of such information. Therefore, foreign government information shall be classified at least Confidential, but higher whenever the damage criteria of paragraph 1-501 or 1-502 are determined to be met.

11-101 Duration of Classification

a. Foreign government information is exempt from the automatic declassification and twenty-year systematic review requirements of Chapter III.

b. Unless guidelines developed pursuant to paragraph 11-201 prescribe dates or events for declassification or for review for declassification:

1. Foreign government information shall not be assigned a date or event for automatic declassification unless specified or agreed to by the foreign entity.

2. Foreign government information classified by the Department of Defense on or after December 1, 1978 shall be assigned a date for review for declassification at thirty years from the time the information was originated by the foreign entity, or acquired or classified by the Department of Defense, whichever is earlier. Such information received undated shall be dated upon receipt. The provisions of paragraphs 1-600c.3. and 2-301 are applicable to this body of information.

DECLASSIFICATION

11-200 Policy

In weighing the need to protect information against the possible public interest in disclosure as prescribed in paragraph 3-102, officials shall respect the intent of this Regulation to protect foreign government information and confidential foreign sources.

11-201 Systematic Review

a. By December 1, 1979, the Secretary of Defense shall, in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned, develop systematic review guidelines for thirty-year old foreign government information in the possession or under the control of the Department of Defense. These guidelines shall be kept current through review by the Secretary of Defense at least once every two years unless earlier review for revision is requested by the Archivist of the United States. The senior Department of Defense official having responsibility for the Information Security Program pursuant to paragraph 13-200 shall perform administrative functions necessary to effect such review by the Secretary. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the Secretary of Defense, be used by any agency having custody of the information.

b. Thirty-year old foreign government information shall be reviewed in accordance with guidelines developed under subparagraph a. If, after applying the guidelines to this information, the reviewer determines that continued classification would be appropriate, the reviewer shall submit a recommendation for extension to the Secretary of Defense or the Secretary of the appropriate Military Department.

c. The Secretary of Defense and the Secretaries of the Military Departments may extend the classification of foreign government information beyond thirty years when, in accordance with the provisions of this Regulation, such extension is warranted. This authority may not be delegated. When classification is extended beyond thirty years, a date no more than ten years later may be set for declassification or for the next review. That action and date shall be marked on the document. Subsequent reviews for declassification shall be set at no more than ten-year intervals unless a longer interval has been authorized pursuant to paragraph 3-200.

11-202 Mandatory Review

Requests for mandatory review for declassification of foreign government information shall be processed and acted upon in accordance with the

provisions of Section 3 of Chapter III, except that foreign government information will be declassified only in accordance with the guidelines developed for such purpose and after necessary consultation with other Department of Defense Components or government agencies with subject matter interest. In cases where these guidelines cannot be applied to the foreign government information requested, or in the absence of such guidelines, consultation with the foreign originator through appropriate channels normally should be effected prior to final action on the request. When the responsible Component is knowledgeable of the foreign originator's view toward declassification or continued classification of the types of information requested, consultation with the foreign originator may not be necessary.

Section 3

MARKING

11-300 Equivalent United States Classification Designations

Except for the foreign security classification designation RESTRICTED, foreign classification designations, including those of international organizations of governments i.e., NATO and CENTO, generally parallel United States classification designations. A table of equivalents is contained in Appendix A.

11-301 Marking NATO and CENTO Documents

Classified documents originated by NATO and CENTO, if not already marked with the appropriate classification in English, shall be so marked. Markings required under paragraph 4-402 shall not be placed on documents originated by NATO and CENTO. The date for declassification or review shall be marked on such documents only as required by paragraph 11-201c. Documents originated by NATO and CENTO that are marked RESTRICTED shall be marked with the following additional notation: "To be safeguarded in accordance with _____." In the blank space insert:

For NATO: "USSAN Instruction 1-69" (Promulgated by DoD Instruction C-5210.21)

For CENTO: "USSAC Instruction 1-68" (Promulgated by DoD Instruction C-5210.35)

11-302 Marking Other Foreign Government Documents

a. If the security classification designation of foreign government documents is shown in English, no other classification marking shall be applied. If the foreign classification designation is not shown in English, the equivalent overall United States classification designation

(Appendix A) shall be marked conspicuously on the document. In those cases where foreign government documents are marked with a classification designation having no United States equivalent, as in the last column of Appendix A, such documents shall be marked in accordance with b., below.

b. Certain foreign governments use a fourth classification designation as shown in the last column of Appendix A. Such designations equate to the foreign classification RESTRICTED. If foreign government documents are marked with any of the classification designations listed in the last column of Appendix A, whether or not in English, no other classification marking shall be applied. In all such cases, the notation "This material is to be safeguarded in accordance with paragraph 11-401, DoD 5200.1-R" shall be shown on the face of the document.

c. Dates for declassification or for review for declassification shall be marked on foreign government documents only as required by paragraph 11-201c.

d. Other marking requirements prescribed by this Regulation for United States classified documents are not applicable to documents of foreign governments or international organizations of governments.

11-303 Marking of DoD Classification Determinations

Foreign documents containing foreign government information not classified by the foreign government but provided to the Department of Defense in confidence shall be classified as prescribed in paragraph 11-100b and marked with the appropriate United States classification.

11-304 Marking of Foreign Government Information in DoD Documents

Except where such markings would reveal intelligence information, foreign government information incorporated in Department of Defense documents shall, when practicable, be identified in a manner that ensures that such information is not declassified prematurely or made accessible to nationals of a third country without consent of the originator. This requirement may be satisfied by including the appropriate identification in the portion or paragraph classification markings, e.g., (NATO-S), (U.K.-C), or (FRG-Restricted). All other markings prescribed by paragraph 4-103 of this Regulation are applicable to these documents.

Section 4

PROTECTIVE MEASURES

11-400 NATO and CENTO Classified Information

NATO and CENTO classified information shall be safeguarded in accordance with the provisions of DoD Instruction C-5210.21 (reference (e)) and DoD Instruction C-5210.35 (reference (p)), respectively.

11-401 Other Foreign Government Information

a. Classified foreign government information other than NATO and CENTO information shall be protected as is prescribed by this Regulation for United States classified information of a comparable level.

b. Foreign government information marked under paragraph 11-302b shall be protected as United States CONFIDENTIAL, except that such information may be stored in locked filing cabinets, desks or other similar closed spaces that will prevent access by unauthorized persons.

SPECIAL ACCESS PROGRAMS

12-100 Policy

It is the policy of the Department of Defense to utilize the standard classification categories and the applicable sections of Executive Order 12065 and its implementing Information Security Oversight Office Directive, to limit access to classified information on a "need-to-know" basis to personnel who have been determined to be trustworthy. It is the further policy to apply the "need-to-know" principle in the regular system so that there will be no need to resort to formal Special Access Programs. In this context, Special Access Programs may be created or continued only on a specific showing that:

- a. normal management and safeguarding procedures are not sufficient to limit "need-to-know" or access;
- b. the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and
- c. the special access controls balance the need to protect the information against the full spectrum of needs to use the information.

12-101 Establishment of Special Access Programs

- a. Procedures for the establishment of Special Access Programs involving NATO and CENTO classified information are based on international treaty requirements (references (o) and (p)).
- b. The policies and procedures for access to and dissemination of Restricted Data and Critical Nuclear Weapon Design Information are contained in reference (n).
- c. Special Access Programs for foreign intelligence information under the cognizance of the Director of Central Intelligence or the National Communications Security Committee (NCSC) originate outside the Department of Defense. However, coordination with the Deputy Under Secretary of Defense (Policy) is necessary prior to the establishment or implementation of any such programs by any DoD Component. The information required by paragraph 12-102 will be provided.
- d. Special Access Programs, other than those specified in subparagraphs a., b., and c. above, that the Departments of the Army, Navy, and Air Force desire to establish after the promulgation date of this Regulation, shall be submitted with the information referred to in paragraph 12-102, to the Secretary of the respective Department for approval. If the Secretary of the Military Department approves the

establishment of such program, a copy of the information and rationale for approval shall be furnished to the Deputy Under Secretary of Defense (Policy).

e. Special Access Programs, other than those specified in subparagraph a., b., and c. above, that are desired to be established in any DoD Component other than the Military Departments shall be submitted with the information referred to in paragraph 12-102 to the Deputy Under Secretary of Defense (Policy) for approval.

f. Special Access Programs are required to be reviewed regularly, and all such programs, except those required by treaty or international agreement, shall terminate automatically every five years unless reestablished in accordance with the procedures specified above. DoD Components shall review annually any Special Access Programs they have.

12-102 Reporting on Special Access Programs

Each Special Access Program required to be reported under paragraph 12-101 including each subprogram shall be described in the following manner:

a. Department or Agency _____, and subunit, if applicable;

b. Unclassified name or short title of program;

c. Relationship, if any, to other programs in the DoD or other government agency;

d. Rationale for establishment of the Special Access program. The reason why the normal management and safeguarding procedures for classified information are inadequate must be explained.

e. Estimated number of persons to be granted Special Access.

Number of such persons in requesting department or agency _____
Number of such persons in other DoD Components _____
Number of such persons in non-DoD departments or agencies _____
Total _____

f. Attach a copy of all instructions pertaining to the program security requirements including, but not limited to, those governing access to program information.

12-103 Review, Continuation and Accounting for Special Access Programs

a. Within 180 days after the effective date of this Regulation, heads of DoD Components shall review all existing Special Access Programs under their jurisdiction. Such programs shall be continued only in accordance with the procedures specified in paragraph 12-101 above.

b. The Deputy Under Secretary of Defense (Policy) shall maintain a listing of those special access programs coordinated with his office under paragraphs 12-101c. and 12-101d. above.

12-104 Notification

a. The Secretaries of the Military Departments or their designees and the Deputy Under Secretary of Defense (Policy) for other DoD Components shall, in those Special Access Programs affecting contractors, make the programs applicable by legally binding instruments and provide copies to the Deputy Director, Contract Administration Services (DDCAS), Defense Logistics Agency (DLA).

b. To the extent necessary for DDCAS/DLA to execute its security responsibilities with respect to special access programs under its security cognizance, DDCAS/DLA personnel shall have access to all information relating to the administration of these programs.

CHAPTER XIII
PROGRAM MANAGEMENT

Section 1
EXECUTIVE BRANCH OVERSIGHT AND POLICY DIRECTION

13-100 National Security Council

Pursuant to the provisions of Executive Order 12065 (reference (b)), the National Security Council (NSC) may review all matters with respect to its implementation and shall provide overall policy direction for the Information Security Program.

13-101 Administrator of General Services

The Administrator of General Services is responsible for implementing and monitoring the Information Security Program established pursuant to Executive Order 12065. In accordance with the Order, this responsibility shall be delegated to an Information Security Oversight Office (ISOO).

13-102 Information Security Oversight Office

a. Composition. The Information Security Oversight Office has a full-time Director appointed by the Administrator of General Services with approval of the President. The Director is supported by a staff appointed by the Administrator of General Services.

b. Functions. The Director of the Information Security Oversight Office is charged with the following principal functions that pertain to the Department of Defense:

1. Oversee DoD actions to ensure compliance with Executive Order 12065 and implementing Directives, e.g., reference (c), and this Regulation;
2. Consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the Information Security Program, including appeals from decisions on declassification requests made pursuant to paragraph 3-301;
3. Report annually to the President through the Administrator of General Services and the NSC on the implementation of Executive Order 12065;
4. Review the DoD implementing Regulation (DoD 5200.1-R) and DoD guidelines for systematic declassification review;
5. Conduct on-site reviews of the Information Security Program of each DoD Component that handles classified information; and

6. Require that Department of Defense information classified in violation of Executive Order 12065 be declassified (see paragraph 3-103).

c. Information Requests. The Director of the Information Security Oversight Office is authorized to request information or material concerning the Department of Defense, as needed by the Office in carrying out its functions.

d. Coordination. Heads of DoD Components shall ensure that any significant requirements levied directly on the Component by the Information Security Oversight Office are brought to the attention of the Office of the Deputy Under Secretary of Defense (Policy).

13-103 Interagency Information Security Committee

Pursuant to Executive Order 12065, an Interagency Information Security Committee (IISC) has been established. It is chaired by the Director of the Information Security Oversight Office and is comprised of representatives of the Secretaries of State, Defense, Treasury, and Energy, the Attorney General, the Director of Central Intelligence, the National Security Council, the Domestic Policy Staff, and the Archivist of the United States. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies. The Committee shall meet at the call of the Chairperson or at the request of a member agency and shall advise the Chairperson on implementation of Executive Order 12065. The Deputy Under Secretary of Defense (Policy), or a designee, is the representative of the Secretary of Defense on the Committee.

Section 2 DEPARTMENT OF DEFENSE

13-200 Management Responsibility

a. The Deputy Under Secretary of Defense (Policy) is the senior DoD official having authority and responsibility to ensure effective and uniform compliance with and implementation of Executive Order 12065 and its implementing Directive (references (b) and (c)). As such, the Deputy Under Secretary of Defense (Policy) shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the DoD Information Security Program. The Deputy Under Secretary of Defense (Policy) may approve waivers or exceptions to the provisions of this Regulation to the extent such action is consistent with references (b) and (c).

b. The heads of DoD Components may approve waivers to the provisions of this Regulation only as specifically provided for elsewhere herein.

c. The Director, National Security Agency (NSA), is, pursuant to reference (a), authorized to prescribe such additional internal procedures or requirements that are necessary to achieve conformity with COMSEC and SCI policies and standards. In this regard, the Director, NSA, may approve waivers or exceptions to such additional internal procedures or requirements. However, the authority to lower any COMSEC security standards rests with the Secretary of Defense. Therefore, requests for approval of waivers or exceptions to established COMSEC security standards which, if adopted, will have the effect of lowering such standards, shall be submitted to the Deputy Under Secretary of Defense (Policy) for approval by the Secretary of Defense.

13-201 DoD Information Security Committee

The Department of Defense Information Security Committee (DISC) established pursuant to reference (a) is comprised of the Deputy Under Secretary of Defense (Policy), Chairperson, and representatives of the General Counsel, the Under Secretary of Defense (Research and Engineering), the Assistant Secretary of Defense (Public Affairs), and the Deputy Assistant Secretary of Defense (Administration). Other officials of the Department of Defense may be invited to meet with the Committee on matters of specific interest. The Committee shall:

a. Receive, consider and take action upon all suggestions and complaints with respect to the administration of the Department of Defense Information Security Program not resolved at the Component level;

b. Review and evaluate the effectiveness of the administration of the Information Security Program by DoD Components, developing and recommending new or revised uniform policies, standards, criteria or procedures necessary to meet changing conditions or to correct deficiencies in the Information Security Program; and

c. Meet at the call of the Chairperson and establish its own rules of procedure.

Section 3 DOD COMPONENTS

13-300 General

The head of each Component shall establish and maintain an Information Security Program designed to ensure compliance with the provisions of this Regulation throughout the Component.

13-301 Military Departments

The Secretary of each Military Department shall designate a senior official who shall be responsible for compliance with and implementation of this Regulation within the Department. The Secretaries of the Military Departments shall also designate a senior official to chair an Information

Security Committee that shall have authority and responsibility to perform functions for their respective Military Department similar to those described in paragraph 13-201.

13-302 Other Components

The head of each other Component shall designate a senior official who shall be responsible for compliance with and implementation of this Regulation within their respective Component.

13-303 Program Monitorship

The senior officials designated under paragraphs 13-301 and 13-302 are responsible within their respective jurisdictions for monitoring, inspecting and reporting on the status of administration of the DoD Information Security Program at all levels of activity under their cognizance.

13-304 Field Program Management

Throughout the DoD, each activity shall assign an official to serve as security manager for the activity. This official shall be responsible for administration of an effective Information Security Program in that activity with particular emphasis on security education and training; assignment of proper classifications; downgrading and declassification; and safeguarding.

Section 4 REPORTS REQUIREMENTS

13-400 Reports Requirements

(To be developed as report requirements are specified by the Information Security Oversight Office.)

CHAPTER XIV

ADMINISTRATIVE SANCTIONS

14-100 Individual Responsibility

All personnel, civilian or military, of the Department of Defense are responsible individually for complying with the provisions of this Regulation in all respects.

14-101 Violations Subject to Sanctions

Military and civilian personnel of the Department of Defense are subject to administrative sanctions if they:

- a. Knowingly and willfully classify or continue the classification of information in violation of Executive Order 12065, any implementing directives or this Regulation;
- b. Knowingly, willfully and without authorization disclose information properly classified under Executive Order 12065 or prior orders or compromise properly classified information through negligence; or
- c. Knowingly and willfully violate any other provision of Executive Order 12065, any implementing directive or this Regulation.

Sanctions include but are not limited to warning notice, reprimand, termination of classification authority, suspension without pay, forfeiture of pay, removal or discharge and will be imposed upon any person, regardless of office or level of employment, responsible for a violation specified under this paragraph as determined appropriate in the particular case in accordance with applicable law and regulations of this Department. Nothing in this Regulation prohibits or limits action under the Uniform Code of Military Justice based upon violations of that Code.

14-102 Corrective Action

The Secretary of Defense, the Secretaries of the Military Departments, and the heads of other DoD Components shall ensure that appropriate and prompt corrective action is taken whenever a violation under paragraph 14-101 occurs or repeated administrative discrepancies or repeated disregard of requirements of this Regulation occurs (paragraph 14-103).

14-103 Administrative Discrepancies

Repeated administrative discrepancies in the marking and handling of classified documents and material such as failure to show classification authority, failure to apply internal classification markings and incorrect computation of dates for declassification or other repeated disregard of requirements of this Regulation that are determined not to constitute a

violation under paragraph 14-101 may be grounds for adverse administrative action including warning, admonition, reprimand or termination classification authority as determined appropriate in the particular case, in accordance with applicable policies and procedures.

14-104 Reporting Violations

a. Whenever a violation under paragraph 14-101 occurs, the Director of Information Security, Office of Deputy Under Secretary of Defense (Policy), shall be informed of the date and general nature of the occurrence including the relevant paragraphs of this Regulation, the sanctions imposed, and the corrective action taken. Notification of such violations shall be furnished to the Director of the Information Security Oversight Office in accordance with paragraph 5-504 of reference (b) by the Deputy Under Secretary of Defense (Policy).

b. Any action resulting in unauthorized disclosure of properly classified information that constitutes a violation of the criminal statutes and evidence reflected in classified information of possible violations of Federal criminal law by a DoD employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General shall be the subject of a report processed in accordance with DoD Directive 5210.50, reference (g) and DoD Instruction 5200.22, reference (f).

c. Any action reported under paragraph b., above, shall be reported to the Attorney General by the General Counsel, Department of Defense.

APPENDIX A
Equivalent Foreign and International Pact Organization Security Classifications

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL
Argentina	RESTRICIONADO	SECRETO	CONFIDENTIAL
Australia	TOP SECRET	SECRET	CONFIDENTIAL
Austria	STRENG GEHEIM	GEHEIM	VERSCHLUSS
Belgium (French)	TRES SECRET	SECRET	CONFIDENTIEL
(Flemish)	ZEER GEHEIM	GEHEIM	VERTROUWELIJK
Bolivia	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENTIAL
Brazil	ULTRA SECRETO	SECRETO	CONFIDENTIAL
Cambodia	TRES SECRET	SECRET	SECRET/CONFIDENTIEL
Canada	TOP SECRET	SECRET	CONFIDENTIAL
Chile	SECRETO	SECRETO	RESTRICIONADO
Columbia (two systems)	MUY SECRETO RESTRICIONADO RESERVADO	SECRETO SECRETO	CONFIDENTIAL RESERVADO
Costa Rica	ALTO SECRETO	SECRETO	CONFIDENTIAL
Denmark	YDERST HEMMELIGT	HEMDELIGT	FORTROLIGT
Ecuador	SECRETO SIMO	SECRETO	CONFIDENTIAL
			TIL TUVENESTE BRUG
			RESERVADO
			MUR FÜR DEN DIENSTGEBRAUCH
			DIFFUSION RESTRIKTE REPERTE VERSPREIDUNG

CONFIDENTIAL

SECRET

TOP SECRET

Country

El Salvador	SECRETISMO	SECRETO	CONFIDENTIAL	RESERVADO
Ethiopia	YEMLAZ BIRYU MUSTIR	MUSTIR	KIMKIL	
Finland	KUTUAIN SALAINEN	SALAINEN	HEIKILÄKORTALINEN	VALMUTIKAPAL- VELUKSISAAK- TETIAVAKSI
France	TRES SECRET	SECRET DEFENSE	CONFIDENTIAL DEFENSE	
Germany	STRENG GEHEIM	GEHEIM	VERTRAULICH	RESTRIKTIWE
Greece	AKRIFI ANOPHTON	ANOPHTON	EMPHYTIKON	VS-MUR FÜR DEN DIENSTGEBRAUCH
Guatemala	AUTO SECRETO	SECRETO	CONFIDENTIAL	RESTRIKTIWE XPIEWE
Haiti				RESERVADO
Honduras	SUPER SECRETO	SECRET	CONFIDENTIAL	
Hong Kong	TOP SECRET	SECRETO	CONFIDENTIAL	RESERVADO
Hungary	SEIGORJAN TITKOS	SECRET	CONFIDENTIAL	RESTRICTED
Iceland	ALGJORTI	TITKOS	RIZALMAS	
India	TOP SECRET	TRUNADARNAL		
Indonesia	SANGAT RAHASIA	SECRET CONFIDENTIAL	CONFIDENTIAL	RESTRICTED
Iran	HEKOLI SEHRI هکلی سری	RAHASIA	KAFET JAJAN	TERBATAS
Iraq	SEHRI MALLU سهری مللو (Absolutely secret)	SEHRI سهری (Secret)	KHEILL MAHMANAKH خیلان مدرمانه مکتوم	MAHMANAKH مدرمانه مکتوم (Limited)

Country	TOP SECRET	SECRET	CONFIDENTIAL	
Ireland Gaelic	TOP SECRET AM-SICREIDEACH	SECRET SICREIDEACH	CONFIDENTIAL RÚNDA	RESTRICTED SRIANTA
Israel	SODI מסודר '11b	SODI '11b	SHAMUR '11b	MIGRAL '11b
Italy	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Japan	KIKUSU 機密	OKURI 極密	HI 秘	TOULATSUKAICHU 取扱注意 BUGAIH 市外秘
Jordan	معلومات I 高機密 IKUP FIMIL	معلومات I 高機密 IKUP FIMIL	معلومات II 高機密 SAM KUP FIMIL	معلومات
Korea	TRES SECRET	SECRET	SECRET/CONFIDENTIAL	DIFFUSION RESTREINTE
Laos	TRES SECRET	SECRET	CONFIDENTIAL	
Lebanon	TRES SECRET	SECRET	CONFIDENTIAL	
Luxembourg	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Mexico	SECRETO	SECRETO	CONFIDENTIAL	
Netherlands	ZEER GEHEIM	GEHEIM	CONFIDENTIEL or VERTROUWELIJK	BEENSTAGEHEIM
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Nicaragua	ALTO SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Norway	STRENGT HEMMELIG	HEMMELEG	KONFIDENTIELT	
Pakistan	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Paraguay	ALTO SECRETO	SECRETO	CONFIDENTIAL	RESERVADO

Country	TOP SECRET	SECRET	CONFIDENTIAL
Peru	ESTRICTAMENTE SECRETO	SECRETO	RESERVADO
Philippines	TOP SECRET	SECRET	CONFIDENTIAL
Portugal	MUITO SECRETO	SECRETO	CONFIDENTIAL
Spain	MAXIMO SECRETO	SECRETO	CONFIDENTIAL
Sweden (Red Borders)	HEMELIG	HEMELIG	HEMELIG
Switzerland	(Three languages. TOP SECRET has a registration number to distinguish from SECRET and CONFIDENTIAL.)		
French	SECRET	SECRET	SECRET
German	STRENG GEHEIM	GEHEIM	VERSCHUTZT
Italian	SEGRETO	SEGRETO	SEGRETO
Taiwan	絕對機密	極機密	機密
Thailand	LUB TI SOOD ^ด SECRET	LUB MAX ^ด SECRET	LUB ^ด SECRET
Turkey	OK gizli	gizli	ÖZEL
Union of South Africa	TOP SECRET	SECRET	CONFIDENTIAL
Afrikaans	UITERS GEHEIM	GEHEIM	VERHOUDLIK
United Arab Republic (Egypt)	سري TOP SECRET	سري VERY SECRET	سري SECRET
			RESERVE A L'USAGE EXCLUSIVE RU SERVICE NUR FÜR DIENST- LICHEN GEBRAUCH AD EXCLUSIVO USO DI SERVIZIO 密
			POK PID ^د SECRET
			HIZMET ÖZEL
			RESTRICTED
			SECRET
			سري OFFICIAL

Country	TOP SECRET	SECRET	CONFIDENTIAL
United Kingdom	TOP SECRET	SECRET	CONFIDENTIAL
Uruguay	SECRETO	SECRETO	CONFIDENTIAL
USSR	СОБЕЗПЕЧЕНО СЕКРЕТНО	СЕКРЕТНО	НЕ ПОДЛЕЖАЕТ ОТКАЗУ
Viet Nam	TRÈS SECRET	SECRET	CONFIDENTIAL
French	MIL-MAT	MAT	KIN
Vietnamese			CONFIDENTIAL
			TU MAT

INTERNATIONAL ORGANIZATION	TOP SECRET	SECRET	CONFIDENTIAL	(SEE CHAPTER XI)
NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
CENTO	CENTO TOP SECRET	CENTO SECRET	CENTO CONFIDENTIAL	CENTO RESTRICTED

NOTES: In all instances foreign security classification systems are not exactly parallel to the United States system and exact equivalent classifications cannot be stated. The classifications given above represent the nearest comparable designations which are used to signify degrees of protection and control similar to those prescribed for the equivalent United States classifications.

"ATOMAL" information is an exclusive designation used by NATO to identify "Restricted Data" or "Formerly Restricted Data" information released by the Government of the United States to NATO.



APPENDIX B

GENERAL ACCOUNTING OFFICE OFFICIALS
AUTHORIZED TO CERTIFY SECURITY CLEARANCES

(See 7-105c)

The Comptroller General, his Deputy, and Assistants

The General Counsel and Deputy General Counsel

The Director and Deputy Director, Office of Personnel Management

The Director and Deputy Director, Office of Policy

The Directors, Deputy Directors, Associate Directors, and Assistant

Directors of the following Divisions:

General Government Resources and Economic Development

Resources and Economic Development

Manpower and Welfare

International

International Division Overseas Offices

Director European Branch, Frankfurt, Germany

Director Far East Branch, Honolulu, Hawaii

Manager, Sub Office, Bangkok, Thailand

Transportation and Claims

Procurement and Systems Acquisition

Federal Personnel and Compensation

Logistics and Communications

Financial and General Management Studies

Regional Managers

Atlanta, Georgia

Boston, Massachusetts

Chicago, Illinois

Cincinnati, Ohio

Dallas, Texas

Denver, Colorado

Detroit, Michigan

Kansas City, Missouri

Los Angeles, California

New York, New York

Norfolk, Virginia

Philadelphia, Pennsylvania

San Francisco, California

Seattle, Washington

Washington, D.C. (Falls Church, Virginia)

APPENDIX C

INSTRUCTIONS GOVERNING USE OF
CODE WORDS, NICKNAMES, AND EXERCISE TERMS

(See 7-210)

1. Definitions

a. Using Component. The DoD component to which a code word is allocated for use, and which assigns to the word a classified meaning, or which originates nicknames and exercise terms using the procedure established by the Joint Chiefs of Staff.

b. Code Word. Word selected from those listed in Joint Army, Navy, Air Force Publication (JANAP) 299 and subsequent volumes, and assigned a classified meaning by appropriate authority to insure proper security concerning intentions, and to safeguard information pertaining to actual, real world military plans or operations classified as Confidential or higher. A code word shall not be assigned to test, drill or exercise activities. A code word is placed in one of three categories:

(1) Available. Allocated to the using component. Available code words individually will be unclassified until placed in the active category.

(2) Active. Assigned a classified meaning and current.

(3) Cancelled. Formerly active, but discontinued due to compromise, suspected compromise, cessation or completion of the operation to which the code word pertained. Cancelled code words individually will be unclassified and remain so until returned to the active category.

c. Nickname. A combination of two separate unclassified words which is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

d. Exercise Term. A combination of two words normally unclassified used exclusively to designate a test, drill or exercise. An exercise term is employed to preclude the possibility of confusing exercise directions with actual operations directives.

2. Policy and Procedure

a. Code Words. The Joint Chiefs of Staff are responsible for allocating words or blocks of code words from JANAP 299 to DoD components. DoD components may request allocation of such code words as required and may reallocate available code words within their organizations, in accordance with individual policies and procedure, subject to applicable rules set forth herein.

(1) A permanent record of all code words shall be maintained by the Joint Chiefs of Staff.

(2) The using component shall account for available code words and maintain a record of each active code word. Upon being cancelled, the using component shall maintain the record for two years; thence the record of each code word may be disposed of in accordance with current practices, and the code word returned to the available inventory.

b. Nicknames

(1) Nicknames may be assigned to actual, real world events, projects, movement of forces, or other nonexercise activities involving elements of information of any classification category, but the nickname, the description or meaning it represents, and the relationship of the nickname and its meaning must be unclassified. A nickname is not designed to achieve a security objective.

(2) Nicknames, improperly selected, can be counterproductive. A nickname must be chosen with sufficient care to ensure that it does not:

(a) Express a degree of bellicosity inconsistent with traditional American ideals or current foreign policy;

(b) Convey connotations offensive to good taste or derogatory to a particular group, sect, or creed; or,

(c) Convey connotations offensive to our allies or other Free World nations.

(3) The following shall not be used as nicknames:

(a) Any two-word combination voice call sign found in JANAP 119 or Allied Communications Publication (ACP) 119. (However, single words in JANAP 119 or ACP 119 may be used as part of a nickname if the first word of the nickname does not appear in JANAP 299 and subsequent volumes.)

(b) Combination of words including word "project," "exercise," or "operation."

(c) Words which may be used correctly either as a single word or as two words, such as "moonlight."

(d) Exotic words, trite expressions, or well-known commercial trademarks.

(4) The Joint Chiefs of Staff shall:

(a) Establish a procedure by which nicknames may be authorized for use by DoD components.

(b) Prescribe a method for the using components to report nicknames used.

(5) The heads of DoD components shall:

(a) Establish controls within their organizations for the assignment of nicknames authorized under subparagraph (4)(a) above.

(b) Under the procedures established, advise the Joint Chiefs of nicknames as they are assigned.

c. Exercise Term

(1) Exercise terms may be assigned only to test, drills or exercises for the purpose of emphasizing that the event is a test, drill or exercise and not an actual real world operation. The exercise term, the description or meaning it represents, and the relationship of the exercise term and its meaning can be classified or unclassified: A classified exercise term is designed to simulate actual use of DoD code words and must be employed using identical security procedures throughout the planning, preparation and execution of the test, drill or exercise to ensure realism.

(2) Selection of exercise terms will follow the same guidance as contained in paragraphs 2.b.(2) and (3) above.

(3) The Joint Chiefs of Staff shall:

(a) Establish a procedure by which exercise terms may be authorized for use by DoD components.

(b) Prescribe a method for using components to report exercise terms used.

(4) The heads of DoD components shall:

(a) Establish controls within their organizations for the assignment of exercise terms authorized under subparagraph (3) above.

(b) Under the procedures established, advise the Joint Chiefs of Staff of exercise terms as they are assigned.

3. Assignment of Classified Meanings to Code Words

a. The DoD component responsible for the development of a plan or the execution of an operation shall be responsible for determining whether to assign a code word.

b. Code words shall be activated for the following purposes only:

- (1) To designate a classified military plan or operation;
- (2) To designate classified geographic locations in conjunction with plans or operations referred to in (1) above; or,
- (3) To conceal intentions in discussions and messages or other documents pertaining to plans, operations, or geographic locations referred to in (1) and (2) above.

c. The using component shall assign to a code word a specific meaning classified Top Secret, Secret, or Confidential, commensurate with military security requirements. Code words shall not be used to cover unclassified meanings. The assigned meaning need not in all cases be classified as high as the classification assigned to the plan or operation as a whole.

d. Code words shall be selected by each using component in such manner that the word used does not suggest the nature of its meaning.

e. A code word shall not be used repeatedly for similar purposes; i.e., if the initial phase of an operation is designated "Meaning," succeeding phases should not be designated "Meaning II" and "Meaning III," but should have different code words.

f. Each DoD component shall establish policies and procedures for the control and assignment of classified meanings to code words, subject to applicable rules set forth herein.

4. Notice of Assignment, Dissemination, and Cancellation of Code Words and Meanings

a. The using component shall promptly notify the Joint Chiefs of Staff when a code word is made active, indicating the word, and its classification. Similar notice shall be made when any changes occur, such as the substitution of a new word for one previously placed in use.

b. The using component is responsible for further dissemination of active code words and meanings to all concerned activities, to include classification of each.

c. The using component is responsible for notifying the Joint Chiefs of Staff of cancelled code words. This cancellation report is considered final action, and no further reporting or accounting of the status of the cancelled code word will be required.

5. Classification and Downgrading Instructions

a. During the development of a plan, or the planning of an operation by the headquarters of the using component, the code word and its meaning shall have the same classification. When dissemination of the plan to other DoD components or to subordinate echelons of the using component is required, the using component may downgrade the code words assigned below the classification assigned to their meanings in order to facilitate additional planning implementation, and execution by such other components or echelons. To facilitate this planning code words shall not be downgraded below Confidential.

b. A code word which is replaced by another code word due to a compromise or suspected compromise, or for any other reason, shall be cancelled, and classified Confidential for a period of two years, after which the code word will become Unclassified.

c. When a plan or operation is discontinued or completed, and is not replaced by a similar plan or operation but the meaning cannot be declassified, the code word assigned thereto shall be cancelled and classified Confidential for a period of two years, or until the meaning is declassified, whichever is sooner, after which the code word will become Unclassified.

d. In every case, whenever a code word is referred to in documents, the security classification of the code word shall be placed in parentheses immediately following the code word, i.e., "Label (C)."

e. When the meaning of a code word no longer requires a classification, the using component shall declassify the meaning and the code word and return the code word to the available inventory.

6. Security Practices

a. The meaning of a code word may be used in a message or other document, together with the code word, only when it is essential to do so. Active code words may be used in correspondence or other documents forwarded to addressees who may or may not have knowledge of the meaning. If the context of a document contains detailed instructions or similar information which indicates the purpose or nature of the related meaning, the active code word shall not be used.

b. In handling correspondence pertaining to active code words, care shall be used to avoid bringing the code words and their meanings together. They should be handled in separate card files, catalogs, indexes, or lists, enveloped separately and dispatched at different times so they do not travel through mail or courier channels together.

c. Code words shall not be used for addresses, return addresses, shipping designators, file indicators, call signs, identification signals, or for other similar purposes.

7. All code words formerly categorized as "inactive" or "obsolete" shall be placed in the current cancelled category and classified Confidential. Unless otherwise restricted, all code words formerly categorized as "cancelled" or "available" shall be individually declassified. All records associated with such code words may be disposed of in accordance with current practices, provided such records have been retained at least two years after the code words were placed in the former categories of "inactive," "obsolete," or "cancelled."

APPENDIX D

FEDERAL AVIATION ADMINISTRATION AIR TRANSPORTATION
SECURITY FIELD OFFICES

(See 8-302a.1)

<u>CITY</u>	<u>STATE</u>
Anchorage	Alaska
Atlanta	Georgia
Baltimore	Maryland
Boston	Massachusetts
Chicago (O'Hare)	Illinois
Cleveland	Ohio
Dallas	Texas
Denver	Colorado
Detroit	Michigan
Honolulu	Hawaii
Houston	Texas
Kansas City	Missouri
Las Vegas	Nevada
Los Angeles	California
Miami	Florida

Minneapolis	Minnesota
Newark	New Jersey
New Orleans	Louisiana
New York (John F. Kennedy)	New York
New York (La Guardia)	New York
Philadelphia	Pennsylvania
Pittsburgh	Pennsylvania
Portland	Oregon
Saint Louis	Missouri
San Antonio	Texas
San Diego	California
San Francisco	California
San Juan	Puerto Rico
Seattle	Washington
Tampa	Florida
Tucson	Arizona
Washington (Dulles)	Washington, D.C.
Washington (National)	Washington, D.C.

ENCLOSURE 1

References

- (d) DoD Directive 5230.9, "Clearance of Department of Defense Public Information," dated December 24, 1966
- (e) DoD Directive C-5200.5, "Communications Security (U)," dated April 13, 1971
- (f) DoD Instruction 5200.22, "Reporting of Security and Criminal Violations," dated July 19, 1978
- (g) DoD Directive 5210.50, "Investigation of and Disciplinary Action Connected with Unauthorized Disclosure of Classified Defense Information," dated April 29, 1966
- (h) DoD Directive 5210.8, "Policy on Investigation and Clearance of DoD Personnel for Access to Classified Defense Information," dated February 15, 1962 (Reprint January 8, 1975)
- (i) DoD Directive 5400.4, "Provision of Information to Congress," dated January 30, 1978
- (j) DoD Directive 7650.1, "General Accounting Office Comprehensive Audits," dated July 9, 1958
- (k) DoD Directive 5220.22, "Department of Defense Industrial Security Program," dated December 1, 1976
- (l) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," dated December 31, 1976
- (m) DoD Directive 5200.15, "Control of Dissemination of Foreign Intelligence," dated January 26, 1976
- (n) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," dated January 12, 1978
- (o) DoD Instruction C-5210.21, "Implementation of NATO Security Procedure (U)," dated December 17, 1973
- (p) DoD Instruction C-5210.35, "Implementation of CENTO Security Regulation (U)," dated June 7, 1968
- (q) DoD Directive 5400.7, "Availability to the Public of DoD Information," dated February 14, 1975
- (r) DoD Instruction 7230.7, "User Charges," dated July 18, 1973
- (s) DoD Directive 5220.6, "Industrial Personnel Security Clearance Program," dated December 20, 1976.
- (t) Joint Army-Navy-Air Force Publication (JANAP) #119 (G), November 1976 and #299, September 1971
- (u) Allied Communication Publications (ACP) #119A, August 1970
- (v) National Security Agency KAG I-D, December 1967
- (w) DoD Directive 5535.2, "Secrecy of Certain Inventories and Withholding of Patent; Delegation of Authority to Secretaries of Army, Navy, and Air Force," dated September 30, 1966
- (x) DoD Directive 5200.12, "Security Measures, Approval and Sponsorship for Scientific and Technical Meetings Involving Disclosure of Classified Information," dated March 7, 1967
- (y) DoD Directive 5000.7, "Official Temporary Duty Travel Abroad," dated June 14, 1977

- (z) DoD Directive 5400.10, "Office of the Secretary of Defense/ Organization of the Joint Chiefs of Staff Implementation of the DoD Freedom of Information Program," dated January 6, 1976
- (aa) DoD 5220.22-R, "Industrial Security Regulation," dated April 1975
- (ab) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," dated October 1977
- (ac) DoD Directive 5210.56, "Use of Force by Personnel Engaged in Law Enforcement and Security Duties," dated May 6, 1969
- (ad) DoD Directive 5400.11, "Personal Privacy and Rights of Individuals Regarding Their Personal Records," dated August 4, 1975
- (ae) National COMSEC Instruction 4005, dated 22 August 1973
- (af) DoD Directive 3224.3, "Physical Security Equipment; Assignment of Responsibility for Research, Development, Test and Evaluation," dated December 1, 1976
- (ag) DoD instruction 1000.13, "Identification Cards for Issue to the Members of the Armed Forces, Their Dependents & Other Qualified Personnel," dated May 23, 1972
- (ah) DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," dated
- (ai) DoD Directive 5030.47, "National Supply System," dated May 27, 1971
- (aj) DoD Directive 4540.1, Operating Procedures for the United States Military Aircraft Over the High Seas," dated June 23, 1962
- (ak) DoD Directive 5210.41, "Security Criteria and Standards for Protecting Nuclear Weapons," dated September 10, 1976
- (al) DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," dated December 18, 1972
- (am) DoD 5200.28-M, "ADP Security Manual: Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems, dated January 1973
- (an) National Communications Security Committee (formerly USCSB) Policy Directive 14-2, dated 1 May 1974
- (ao) DoD 5200.1-I, "DoD Index of Security Classification Guides"

*Published on a semiannual basis.

